PEO EIS
ENTERPRISE INFORMATION SYSTEMS
DEPARTMENT OF THE NAVY

NGEN
NEXT GENERATION ENTERPRISE NETWORK

ITSM Process Interface Document

A Document of High Level ITSM Process Designs for the NGEN Program

Prepared by

ITSM COE

April 23, 2009

This page intentionally left blank.

Executive Summary

This NGEN ITSM Process Interface Document (PID) contains IT Service Management (ITSM) process specifications designed to integrate NGEN objectives with the ITIL v3 framework. It defines the ITSM approach for NGEN that aligns with the selected sourcing model.

Information in this document will provide inputs for the NGEN Statement of Work (SOW) and will serve as the reference document for NGEN process design teams tasked with scoping and refining ITSM processes down to the C-Level as described in figure 1 below.

In this document, all but a few processes are described using a high level process model (flow chart), key seams and interfaces, roles and performance metrics and notes about tool interfaces.

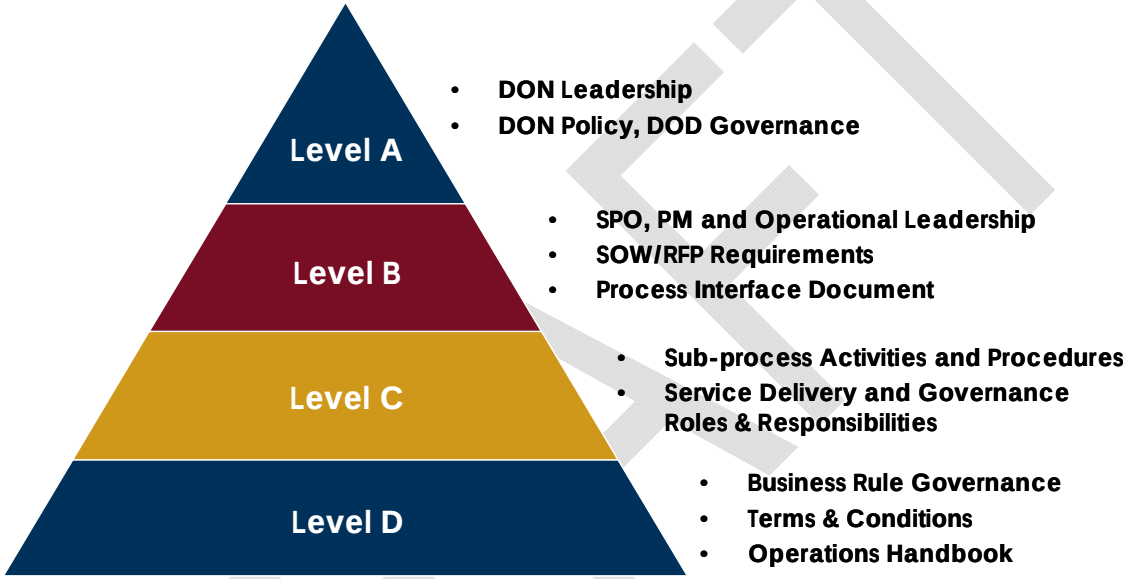


Figure 1 Process Design Pyramid

Document Control

This page provides details on the document file name and location, and its control information.

File Information

File Name and Location	https://portal.peoeis.navy.mil/sites/itsm/Document%20Library/Forms/AllItems.aspx?RootFolder=%2fsites%2fitsm%2fDocument%20Library%2fProcesses%20and%20Procedures%2f000%20Process%20Interfaces

Document Information

Version	2.3	**Original Author**	See Revision History Archive
Status		**Released by**	
Reference	NGEN	**Date Released**	Refer to cover page

Revision History

Version	Date	Author	Group	Change
0.01-0.23	To 03/06/2009	Multiple	Various	Refer to the appendix on Revision History Archive for details on the development of this PID. Note that an early PID v1.1 was re-versioned to 0.09.
0.3	03/16/2009	Multiple	ITSM COE	Revision of Service Transition and CSI Revision of Service Operations Revision of Service Design Revision of Service Strategy
2.0	04/1/2009	Courtney Francis Ashley Amjad	ITSM COE	Consolidation of v0.3 documents, improved CSFs and KPIs, seam tables. Due to earlier discrepancies of versioning, 1.x has been bypassed.
2.1	4/15/09	Courtney L. Francis	ITSM COE	Inserted NGEN Specifications table. Removed assumptions
2.2	4/23/09	Courtney L. Francis Scott Hales	ITSM COE	Updated Executive Summary and Introduction. Posted copy to Portal
2.3	4/24/09	Courtney L. Francis Scott Hales	ITSM	Further revised language in the Executive Summary and Intro.
2.4	5/18/2009	Courtney L. Francis Scott Hales	ITSM	Released to SEI IPT for WBS effort.

Document Approval

This is the sign-off page approving the document and authorizing its release.

SE&I IPT

Name, Title, Program	*Date*
Name, Title, Program	*Date*
Name, Title, Program	*Date*
Name, Title, Program	*Date*
Name, Title, Program	*Date*

NGEN FITT

Name, Title, Program	*Date*
Name, Title, Program	*Date*
Name, Title, Program	*Date*
Name, Title, Program	*Date*
Name, Title, Program	*Date*

Table of Contents

1 Introduction

1.1 Purpose of Document

The main purpose of this Process Interface Document (PID) is to serve as an information document for the Information Technology Service Management (ITSM) process contract requirements in the NGEN Statement of Work (SOW) and Request for Proposal (RFP). It also becomes the foundational information and starting point for NGEN's process design teams who will be architecting what the procedures, roles and technology the Government will need to ensure standard ITSM operations across the NGEN enterprise.

1.2 Objectives

The objectives of this PID are to:

- Document NGEN IT Service Management (ITSM) process specifications to support the NGEN Statement of Work (SOW) and Request for Proposal (RFP)
- Provide ITSM specifications that serve as a starting point for NGEN's ITSM Processes Development teams. This information represents what is defined as the B Level details in the Process Design Pyramid (see figure 1 above)

1.3 Scope

Originally chartered by the NGEN Service Specification (SS) team to address Service Provider seam issues, the ITM Center of Excellence team has developed this document to serve as the reference document for process design teams tasked with scoping and refining processes to an operational level.

The PID is based on the ITIL V3 framework and provides high level process flows, sub-process descriptions, roles and responsibilities, and process specifications critical to the NGEN service model. This PID references the five ITIL volumes and the NGEN Requirements document.

This document is organized under the headings: Service Strategy, Service Design, Service Transition, Service Operations and Continual Service Improvement, as illustrated below.

Figure 2 ITSM Processes and Functions

Service Strategy provides guidance on the design, development, and implementation of service management at a strategic level and is composed of processes for: Service Portfolio Management, Service Financial Management and Demand Management.

Service Design translates strategic plans and objectives, developed in Service Strategy and creates designs and specifications for execution through Service Transition and Service Operation. Process areas covered under Service Design include: Service Catalog Management, Service Level Management, Capacity Management, Availability Management, Information Security Management, IT Service Continuity Management, and Supplier Management.

Service Transition takes the output of the Service Design and develops and improves capabilities for transitioning new and changed services into operation. Process areas covered under Service Transition include: Change Management, Service Asset & Configuration Management, Release & Deployment Management, Transition Planning & Support, Service Validation & Testing, Evaluation, and Knowledge Management.

Service Operation is the realization of the Service Strategy and Service Design and focuses on delivering and maintaining services day to day. Process areas under Service Operation include: Incident Management, Problem Management, Access Management, Event Management, and Request Fulfillment.

Underlying each process is **Continual Service Improvement** as well as several ITIL functions, namely IT Operations Management, Application Management, Technical Management, and the Service Desk. These sections apply across the entire ITSM Lifecycle.

Roles and Responsibilities are generally grouped under the following headings, although other roles may be included in a given process:

- **Process Owner** is the strategic role accountable for achieving standardized and repeatable process performance. There is only ONE Enterprise owner for each process.
- **Process Manager** is the tactical role that performs cross-segment coordination and runs the day-to-day, end-to-end implementation of a process. There is only ONE Enterprise Manager for each process.
- **Service Provider Lead** is the operational role that coordinates activities and supervises resources in the performance of process activities within their segment. There is only ONE Lead for each process within each segment.

Governance

The following table lists the four primary activities responsible for governing each of the ITSM processes, including the key roles described above and their authority in terms of RACI (Responsible, Accountable, Consulted, Informed).

Governance	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead
Establish Process Standards	Sponsor / Lead process design to ensure that the process, tools, and policies are fit for purpose and meets the needs of all stakeholders (enterprise wide, including segment/service providers)	AR	R	CI
	Ensure that all NGEN stakeholders (enterprise wide) who are responsible for performing process procedures understand and are capable of performing their role in the process	AR	R	R
	Provide training and support for customers/users and providers/suppliers on the proper use of ITSM procedures and tools	A	R	R
	Interface with line management, ensuring that the process receives the necessary staff resources.	AR	R	R
Process Performance Management	Define the Key Performance Indicators (KPI) to evaluate the effectiveness and efficiency of the process	AR	R	CI
	Generate reports on KPI reflecting overall performance management	AR	R	I
	Review KPIs and take action required to established required levels or process performance (process adoption and adherence)	AR	R	CI
	Address any issues with the running of the process	AR	R	CI
Continual Process	Improve the effectiveness and efficiency of the process through process modifications	AR	R	CI

Improvement	Review any proposed enhancements or improvements to the process	AR	R	CI
	Provide input to the ongoing Service Improvement Plan	AR	R	R
	Negotiate with segment / service providers on process improvements (contract modifications)	AR	CI	I

1.4 References

NGEN *Requirements Document*, Version 2.0, March 2008.

NGEN Network Operations (NetOps) Concept of Operations (CONOPS), April 2008

NGEN *ITSM COE Charter*, October 2008.

ITIL *Service Strategy*, Office of Government Commerce, TSO: 2007.

ITIL *Service Design*, Office of Government Commerce, TSO: 2007.

ITIL *Service Transition*, Office of Government Commerce, TSO: 2007.

ITIL *Service Operations*, Office of Government Commerce, TSO: 2007.

ITIL *Continual Service Improvement*, Office of Government Commerce, TSO: 2007.

1.5 Assumptions

The process flows described in this document are meant to be high-level models depicting the essential sequence of sub-processes to avoid potentially complex variations. The models are baseline guides that will be used for further process development.

The full authority matrix of each process has not been determined to date. This involves establishing the groups, functions and roles accountable and responsible for the processes and sub-processes. There are still charters and strategies under development that could affect this document.

Service Level Management

The scope of this document does not include the development of Service Level Agreements (SLAs). The SLAs will be defined in the Key Performance Parameters (KPPs), Key Service Attributes (KSAs) and Key Performance Indicators (KPIs) for each service (See NGEN Block 1 Increment 1 Service Specification).

1.6 Risks

To date, a list of risks relating to ITSM strategy have been identified and formally elevated to Leadership which could have an impact on the NGEN initiative and, to a lesser extent, this document.

2 Service Strategy

Service Strategy focuses on the principles underpinning the practice of Service Level Management that are useful for developing service management policies, guidelines and processes across the ITIL Service Lifecycle. Key areas in this volume are: Strategy Generation, Demand Management, Financial Management and Service Portfolio Management.

2.1 Strategy Generation

2.1.1 Process Overview

The Strategy Generation process provides strategic planning guidance on how to design, develop, and implement IT Service Management as a strategic organizational asset. Strategy Generation is a conceptual process that helps guide an organization towards achieving better alignment between business needs and IT services, and the development and optimal utilization of IT resources and capabilities.

Key Objectives of the Strategy Generation process are:

- Determining what service to offer and to whom
- Identifying how value can be created for the customer as well as how to capture it for the organization's stakeholders
- Providing financial visibility and control over value creation
- Defining service quality
- Choosing from among alternatives the best path to improved service quality
- Allocating resources efficiently across the Service Portfolio

Strategy Generation is a conceptual process that utilizes information and performance measurement results from all areas of the organization, including all of the ITIL processes and functional areas, as well as business unit performance. The overarching goal of this process is to achieve optimal alignment between business needs and IT services.

Note that the ITIL process of Strategy Generation is intended to provide IT service management guidance for senior business and IT executives to incorporate into the organization's overall strategic planning process. There is no formal ITIL process model for developing an organization's strategy, as widely divergent models exist depending on the vision, culture, and size of the organization, as well as the industry(s) in which the organization operates.

However, Strategy Generation is intended to be considered as best practice guidance in helping an organization achieves the following two prominent goals of the ITIL v3 framework:

- Congruity between business needs and IT services (Business & IT Alignment)
- Optimization of the organization's portfolio of IT investments (Service Portfolio optimization)

The following known tool interfaces requirements should be considered during further development of the process:

- Service Knowledge Management System (SKMS)
- Financial Management System (ERP, etc.).

2.2 Demand Management

2.2.1 Process Overview

Demand Management is the set of activities utilized to understand and influence customer demand for services and guide the provision of capacity to meet these demands. This process is primarily responsible for synchronizing consumption (demand) with the capacity (supply) of IT resources. At a strategic level Demand Management can involve analysis of patterns of business activity and user profiles. At a tactical level it can involve use of differential charging and other incentives to encourage customers to use IT Services at less busy times.

Key Objectives of Demand Management are:

- Identification, analysis, and codification of Patterns of Business Activities (PBA).
- Organizing services into Core and Supporting packages
- Packaging services based on demand
- Planning and providing system capacity and availability.
- Monitoring and reporting system performance
- Modeling and forecasting system performance

Demand Management is a critical aspect of service management and is tightly coupled with Capacity Management. Demand Management seeks to optimize the use of capacity (and minimize cost of capacity provisioning) by proactively managing customer utilization of IT services by shifting peak workloads to less utilized times, servers or places.

In summary, Demand Management comprises two primary activities (demand analysis and demand shaping):

- Demand Analysis: Identification and analysis of Patterns of Business Activity (PBA) and user profiles that generate demand.
- Demand Shaping: Utilizing techniques to influence and manage demand in such a way that excess capacity is reduced but the business and customer requirements are still satisfied.

Demand management works in close collaboration with Capacity Management, Service Portfolio Management, and Financial Management.

2.2.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

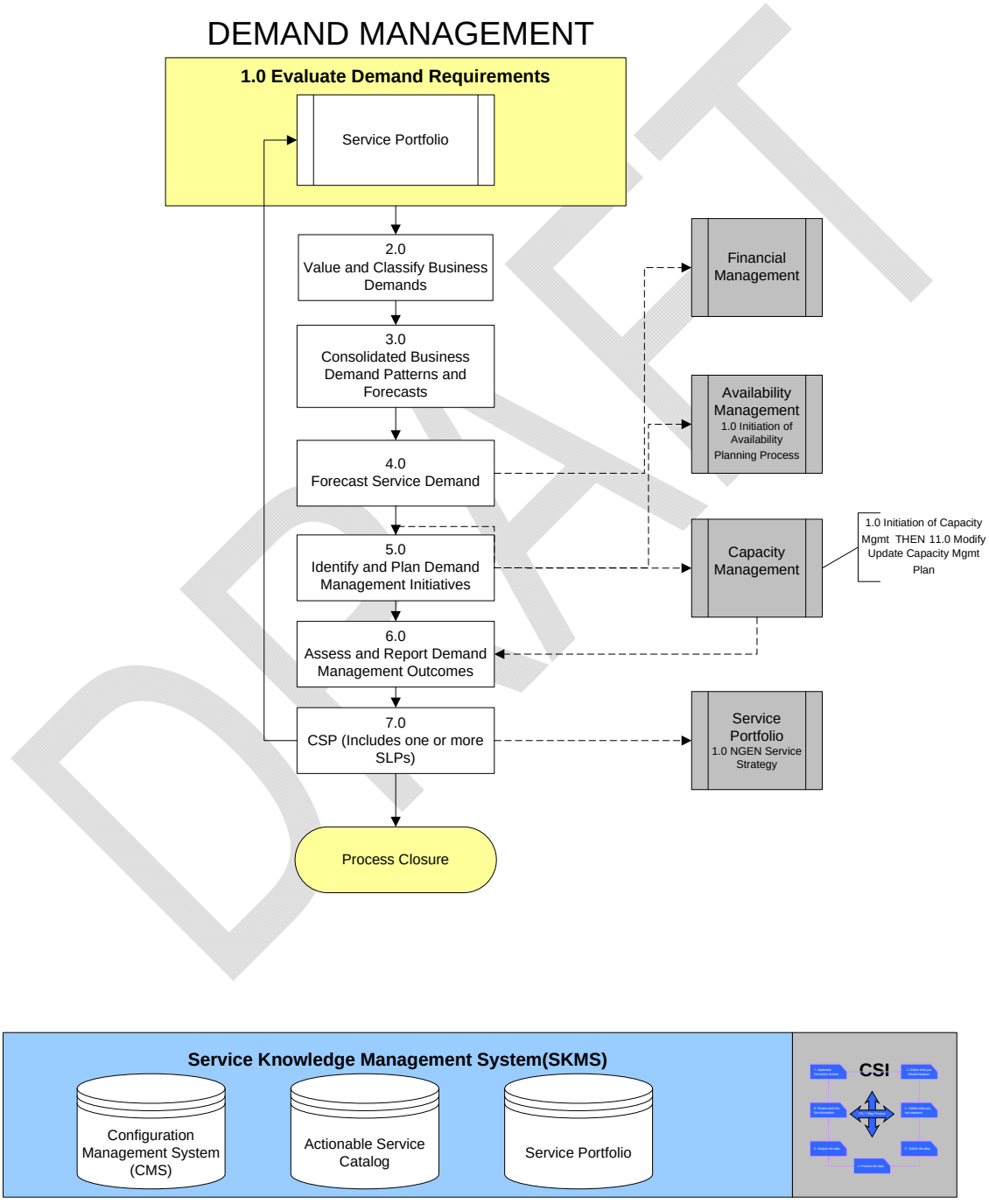


Figure 3 Demand Management Model

2.2.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Evaluate Demand Requirements	Evaluate patterns of the end-user behaviors and relate those patterns to synchronize the consumption (demand) with the capacity (supply) of IT resources.
2.0	Value & Classify Business Demands	Define a value-driven classification scheme for NGEN demands and establish a set of criteria based on criticality or other predetermined criteria.
3.0	Consolidate Business Demand Patterns of Forecasts	Collect NGEN demand patterns and forecast demand.
4.0	Forecast Service Demand	Produce detailed demand forecasts to be utilized in capacity planning.
5.0	Identify and Plan Demand Management Initiatives	Identify service demand patterns.
6.0	Assess & Report Demand Management Outcomes	Baseline service demand patterns.
7.0	CSP (include one or more SLP)	Analyze service demand. Present the Core Service Package (CSP) to describe in detail the core service that may be shared by tow or more Service Level Packages (SLP).

2.2.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate the required ITSM process specifications with seams and key roles.

Seam	Required ITSM Process Specification
	NGEN will have a single source of record for all Demand Management artifacts (i.e. forecasts, Core Services Packages.)

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager (Enterprise Demand Manager)	Service Provider Lead	Business Relationship Manager
	Establish a clear value-driven classification scheme for business demands (e.g. mission critical, operational and discretionary demand.)	CI	AR	R	R
	Baseline service demand patterns to identify significant changes in demand.	CI	AR	R	R
	Forecast patterns of business activity based on location, volume, frequency, and duration.	CI	AR	R	R
	Identify opportunities to optimize demand (reduce spikes in demands and incentives to mold the PBA).	CI	AR	R	R
	Produce a Core Service Package (which may consist of two or more Service Level Packages) for new services after the introduction of a new service or a material change in demand.	CI	AR	R	R

2.2.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Strategy Generation
- Service Portfolio Management

- Financial Management
- Capacity Management
- Supplier Management
- Service Level Management

Inputs

Consider the inputs to the process:

- Analysis of patterns of business activity and user profiles

Outputs

Consider the outputs from the process:

- Demand plan.

2.2.6 Roles

The following roles have been identified with the process.

Roles	Description
Demand Management Process Owner	The strategic role accountable for the Process.
Demand Management Process Manager (Enterprise Demand Manager)	The tactical role that performs cross-segment coordination by analyzing the demand for services for all Customer groups (represented by Business Relationship Managers) and producing demand policies consisting of Core Service Packages (including SLPs) to optimally shape demand with the overall enterprise capacity investment.
Business Relationship Manager	The customer advocate that communicates the forecasted demand and service level package requirements (utility and warranty) required by their Customer for each Service.

2.2.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Accurate Forecasts of Current and	1	Percentage accuracy in predicted demand cycles

	Future IT Service Demand	2	Reduction in capacity and performance related Incidents
2	Effective Demand Management	3	Increased utilization of IT infrastructure
		4	Decrease in idle capacity
		5	Reduction in cost of IT service provision with stable quality levels

2.2.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Service Knowledge Management System (SKMS)
- System Monitoring Tools

2.3 Service Portfolio Management

2.3.1 Process Overview

Service Portfolio Management is responsible for managing and optimizing the value of an organization's complete portfolio of IT services. A Service Portfolio consists of a service provider's ability to deliver services to specific customers and market segments. It is a dynamic method for governing investments in IT Service Management across the enterprise and managing them for long-term value. The Service Portfolio defines, measures, and manages all services according to their defined business value, expressed as:

• Business Value = Utility (Fit-for-Purpose) + Warranty (Fit-for-Use).

Key Objectives of Service Portfolio Management are:

- Defining the inventory of services, ensuring business cases, and validating portfolio data
- Maximizing portfolio value, aligning and prioritizing, and balancing supply and demand
- Finalizing proposed portfolio
- Authorizing services and resources
- Communicating decisions, allocating resources, and chartering services

The Service Portfolio includes all chartered services including new services or changes in the pipeline, active services on the catalog, and retired services:

- Service Pipeline (services that have been proposed or in development).
- Service Catalogue (live services or those available for deployment).
- Retired Services (decommissioned services).

The Service Portfolio is the tangible realization of the organization's strategic objectives and vision for IT as prescribed by Strategy Generation, and is highly dependent on data and analysis

from Demand Management and Financial Management to analyze business cases for IT services and make optimal IT investment decisions.

2.3.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

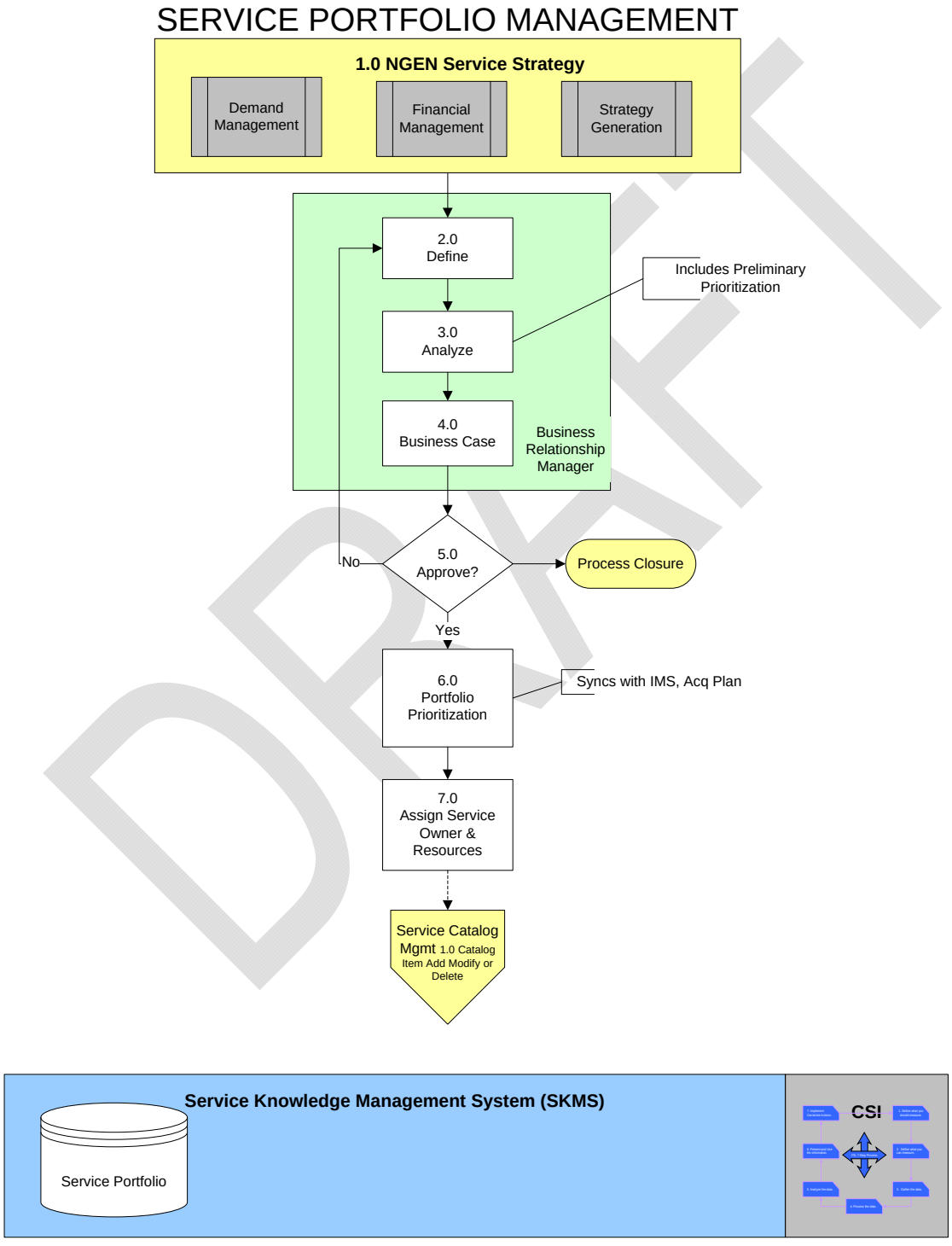


Figure 4 Service Portfolio Management Model

2.3.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Service Strategy	Determine how to design, develop, and implement Service Management for the NGEN Program.
2.0	Define	Define services included in the NGEN Portfolio (inventory services, ensure business cases, and validate portfolio data, considering option space, mission imperatives, compliance, trends, intangible benefits, strategic or business fit, social responsibilities, and innovation).
3.0	Analyze	Maximize portfolio value, align and prioritize, and balance supply and demand.
4.0	Business Case	Long-term goals of the organization, which services are required to meet those goals, and what capabilities and resources are required for the organization to achieve those services?
5.0	Approve?	Following established DoD guidelines, determine budget allocation and categorize as mission critical, growth, discretionary, non-discretionary, or core.
6.0	Portfolio Prioritization	Finalize proposed portfolio by authorizing service(s) and resources. Categorize the outcomes of existing services as either: retain, replace, rationalize, re-factor, renew, or retire.
7.0	Assign Service Owner & Resources	Monitor, measure, reassess, and rebalance investments. Make trade-offs as NGEN needs change. Seek an efficient portfolio with optimal levels of ROI and risk.

2.3.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	NGEN will have a single source of record for all Service Portfolio items. This tool will track Service Portfolio items from initial definition through analysis up to retirement.
	The Government (DON) will establish a clear definition of a request for service and verify that the request has not been previously submitted or reviewed.
	The Government (DON) will assign a Service Owner and appropriate resources to complete the Service Design Package.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager (Enterprise Service Portfolio Manager)	Service Provider Lead	Service Portfolio Management Approval Committee	Service Owner
	Ensures that the process is fit for purpose which includes sponsorship, design, process change management and establishment and monitoring of performance metrics.	A/R	C/I	C/I	C/I	C/I
	Performs cross segment coordination for: business case analysis, requirements, financial analysis, valuation, customer requirements, and statement of works. Ensures that the Service Portfolio is accurate and up-to-date and Process requirements are met.	I	A/R	C	C	C
	For any new services not currently in the Service Catalog, receives and shepherds request for new services through the Service Strategy	C/I	A/R	C	C	C

	processes.					
	Reviews requests for new services (business cases) and approves or rejects and prioritizes new requests.	C/I	C/I	I	A/R	C/I
	Oversees Service Design, Request for Change (RFC) process and transition. Manages the services until retirement.	C/I	C/I	I	C/I	A/R
	Verify that a request has not been previously submitted or reviewed.	C/I	A/R	R	R	R
	Establish clear definition of a request for service in addition to verification that the request has not been previously submitted or reviewed.	CI	AR	R	R	R
	Build a business case for each new IT service request by documenting the risk, cost, benefit, and Return on Investment (ROI).	CI	AR	R	R	R
	Analyze all requests to ensure that investment and portfolio decisions consider the projected values of specific projects and services.	CI	AR	R	R	R
	Evaluate the business case for approval to be included in the Service Portfolio.	CI	AR	R	R	R
	Prioritize approved services based on service strategy needs of the enterprise and its relative value to other portfolio items, available resources, the IMS and budget constraints.	CI	AR	R	R	R
	Manage all IT services throughout the lifecycle until retirement and oversee activities related to Service Design, Service Transition and the Request for Change (RFC) process.	CI	AR	R	R	R
	Ensure that requests for IT services not on the Service Catalog must go through Portfolio Management.	CI	AR	R	R	R

2.3.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Strategy Generation
- Demand Management
- Financial Management
- Service Catalog Management
- Supplier Management
- Capacity Management
- Service Level Management
- Availability Management.

Inputs

Consider the inputs to the process:

- Service Assets
- Current services
- Contract commitments
- New service development
- Continual process improvements on current services.

Outputs

Consider the outputs from the process:

- Service Portfolio
- Value Proposition
- Business Cases
- Priorities
- Risks
- Offerings and Packages
- Cost and pricing models
- Charter.

2.3.6 Roles

The following roles have been identified with the process.

Roles	Description
Service Portfolio Management Process Owner	The strategic role accountable for the Process.
Service Portfolio Management Process Manager	The tactical role that performs cross segment coordination for: business case analysis, requirements, financial analysis, valuation, customer requirements, and statement of works. Ensures that the Service Portfolio is accurate and up-to-date and Process requirements are met.
Service Owner	A role that is accountable for a specific service, overseeing Service Design, Request for Change (RFC) process and transition. The Service Owner manages the service until retirement and is responsible for its continual improvement.
Service Manager	This role manages the development, implementation, evaluations and on-going management of new and existing products and services.
Service Portfolio Approval Committee	Reviews requests for new services (business cases) and approves or rejects and prioritizes new requests.
Business Relationship Manager	The customer advocate that communicates the forecasted demand and service level package requirements (utility and warranty) required by their Customer for each Service.

2.3.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Optimal Portfolio of IT Investments	1	IT spend as a percentage of business revenue/net income
		2	Number of business-critical IT-enabled service customer needs unmet

		3	Percentage total organization's budget devoted to IT spend compared to direct competitors
		4	Percentage customer satisfaction with current IT service offerings (survey results)
2	Strategically Sound Investments in IT Services (Meeting Current and Future Needs of the Business)	5	Percentage of IT spend invested in next-generation technologies (transform the business)
		6	Percentage of IT spend invested in enhancement of existing IT services (grow the business)
		7	Percentage of IT spend invested in maintaining current IT technologies/operations (run the business)
3	Positive Financial Returns from IT Investments	8	Percentage of IT investments resulting in realized positive NPV (net present value)
		9	Percentage of IT investments that meet or exceed ROI (return on investment) targets
		10	Percentage of IT investments that meet or exceed VOI (value of investment) targets

2.3.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Service Catalog/Ordering System
- Service Knowledge Management System (SKMS)

2.4 Financial Management

2.4.1 Process Overview

The Financial Management process provides the business and IT with the quantification (in financial terms) of the value of IT services, the value of the assets underlying the provisioning of those services, and the qualification of operational forecasting. It includes all function and processes responsible for managing an IT service provider's budgeting, accounting and charging policies and activities.

Key objectives of Financial Management are:

- Establishing and enforcing IT financial controls
- Ensuring compliance with legal, industry, and corporate standards and procedures

- Assisting IT portfolio investment decisions by providing detailed business cases as well as financial input for decision support
- Effectively predicting and controlling IT budgets
- Providing the enterprise with operational visibility, insight, and superior decision-making.

The overriding goal of Financial Management is to provide cost effective stewardship of the IT assets and the financial resources used in providing IT services. Primarily this is to enable an organization to account fully for the financial resources consumed by the IT service provider and to attribute these costs to the services delivered to the organization's customers.

This is accomplished by the categorization, collection and analysis of accounting, contract and pricing data including the following typical cost elements:

- Hardware and software license costs
- Annual maintenance fees for hardware and software
- Personnel resources used in the support or maintenance of a service
- Utilities, data centre or other facilities charges
- Taxes, capital or interest charges
- Compliance costs
- Transfer costs and internal charging by other business units/processes.

•

2.4.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here
Process Number: <Fill text in here
Version: <Fill text in here
Last Updated: <Fill text in here

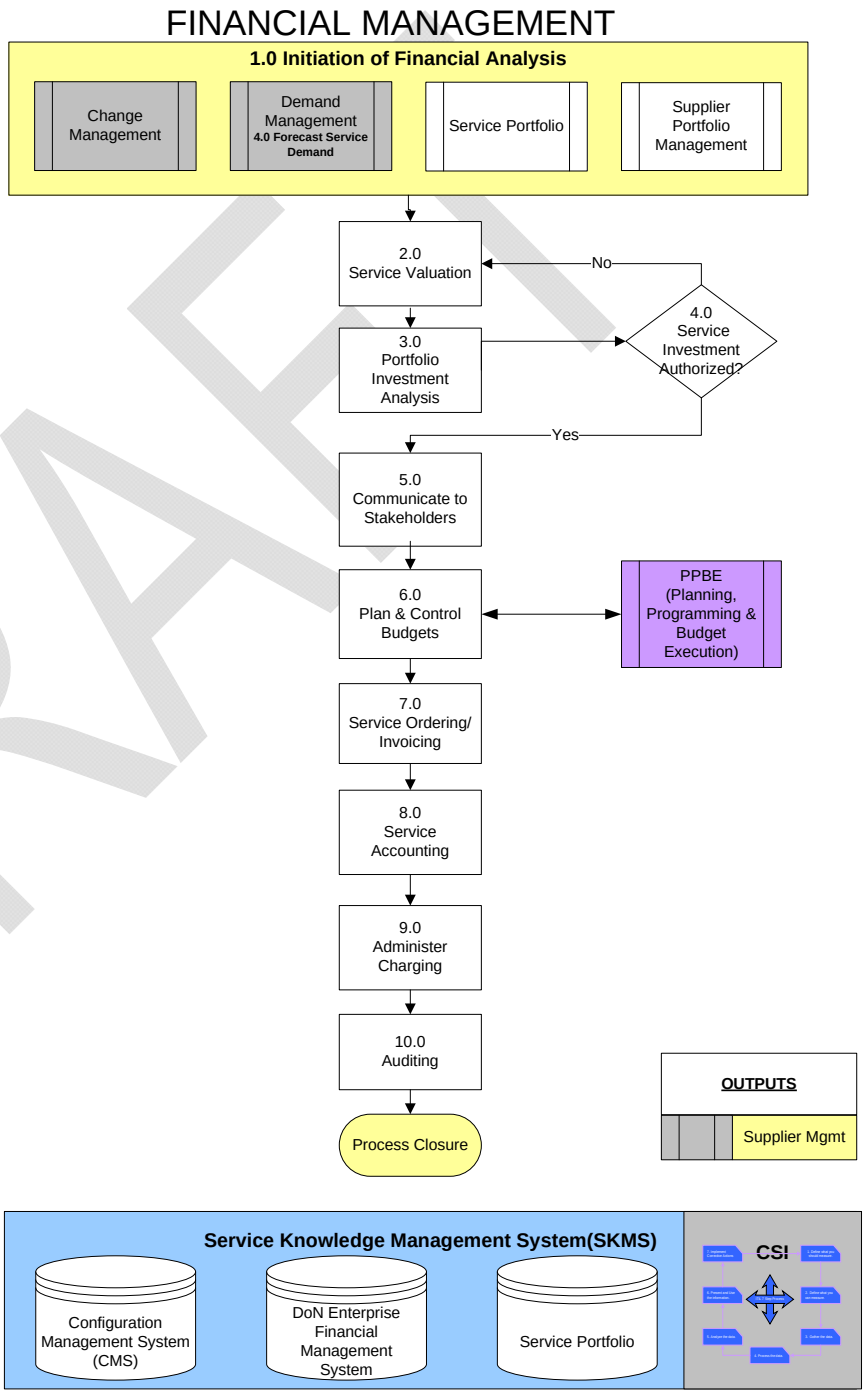


Figure 5 Financial Management Model

2.4.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of Financial Analysis	Assist financial management with managing IT resources using inputs from Change, Demand, Service Portfolio and Supplier Management processes.
2.0	Service Valuation	Quantify (in financial terms), the value of IT Services and the value of the assets underlying the provisioning of those services.
3.0	Portfolio Investment Analysis	Analyze the cost and benefits of the new service(s) under consideration based on impact to the NGEN program, infrastructure, and existing services. Develop business case to support the Service Portfolio Management process.
4.0	Service Investment Authorized?	Determine whether requests for new Service Investments are approved or rejected. The Financial Management Approval Committee (a Government role which is TBD), will allocate financial and workforce resources to approved requests and communicate the authorization to stakeholders. Rejected requests are re-submitted for Service Valuation (Step 2.0).
5.0	Communicate to Stakeholders	Publish budget allocations to customer Business Financial Managers (BFMs) to initiate financial management budgeting process.
6.0	Plan & Control Budgets	Establish budgeting framework based on DoD standards. Align budgetary plants to DoD standards and the PPBE process.
7.0	Service Ordering/ Invoices	Initiate procurement by selecting the appropriate supplier(s) and placing the order. Attribute actual usage data to customers and apply the NGEN pricing model to support invoicing.
8.0	Service Accounting	Track and record all costs incurred in the NGEN program and attribute those costs to NGEN customers. Perform this activity continuously

		throughout the NGEN program.
9.0	Administer Charging	Recover cost of IT services by charging customers for services rendered. Deliver bills to customers for payment based on an established pricing model as defined in NGEN's chargeback framework.
10.0	Auditing	Examine financial data and the Financial Management process to determine level of conformance to NGEN standards and practices. This activity also identifies irregularities and improvement opportunities.

2.4.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	NGEN will determine a "unit price" (e.g. budget allocation, chargeback, etc.) for each Service.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager (NGEN BFM)	Service Provider Lead	Financial Management Approval Committee
	Determine the colors of money and how these can be used to fund Services (e.g.) • Operations & Maintenance	CI	AR	R	R

	(O&M) - 1 year cycle • Research & Development (R&D) - 2 year cycle • Procurement - 3 year cycle				
	Define, calculate and monitor the unit costs of provisioning each Service.	CI	AR	R	R
	Quantify, in financial terms, the value of IT Services and the value of the assets underlying the provisioning of those services.	CI	AR	R	R
	Review requests for new investments and approve or reject the allocation of the budget and resources.	CI	AR	R	R
	Perform periodic and ad- hoc audits to ensure compliance with the NGEN IT Financial Management strategy and adherence to published procedures and policies.	CI	AR	R	R
	Determine the appropriate pricing for IT Services.	CI	AR	R	R
	Update the Government's Asset Management tool upon the procurement or update of a service.	CI	AR	R	R
	Monitor and report costs against the budget, review the financial forecasts, and manage costs accordingly.	CI	AR	R	R

2.4.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Strategy Generation
- Service Portfolio Management
- Demand Management
- Service Level Management
- Supplier Management

- Capacity Management
- Service Asset and Configuration Management.

Inputs

Consider the inputs to the process:

- Service Level Agreements
- Service valuation
- Demand modeling
- Service investment analysis
- Estimated costs and cost types
- Depreciation schedules
- Service Catalog and CIs.

Outputs

Consider the outputs from the process:

- Budget for governance of expenses
- Actual costs of services
- Management reporting to assist decision-making
- Service value potential
- Authorization
- Service Portfolio
- Costing model
- Charging rates and policies per service
- Return on Investment, Return on Capital Employed, and Total Cost of Ownership.

2.4.6 Roles

The following roles have been identified with the process.

Roles	Description
Financial Management Process Owner	The strategic role accountable for the Process.
Financial Management Process Manager (NGEN BFM)	The tactical role that performs cross segment coordination of the quantification, in financial terms, of the value of IT Services and the value of assets underlying the provisioning of those services.

Financial Management Approval Committee	Reviews requests for new investments and approves or rejects the allocation of budget and resources.

2.4.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Provide Effective Stewardship of IT Finances	1	Unplanned Cost Variance. NGEN must provide the Navy and Marine Corps with improved cost planning to inform DON Program Objective decisions and to effectively use allocated budget. = Total to-date planned budget costs minus Total IT budget
		2	Cost Performance Index. NGEN will employ financial resources fully and not exceed planned and authorized budget. = Total to-date planned budget costs divided by Total to-date actual budget costs.
		3	Estimated Year-End Costs. Determine how much will actually be spent at the end of the fiscal year. = Total IT budget multiplied by the Cost Performance Index KPI.
		4	Variance at Budget Year-End. Determine how much will the NGEN program be over or under its fiscal IT budget. = Estimated Year-End Costs KPI minus the Total IT budget.
		6	Financial Management Process Maturity. NGEN will execute financial management to a high-level of process maturity. Evaluated as a COBIT maturity process level.
		8	Number of Financial Reports/Forecasts Delivered Late. The NGEN financial management process will ensure financial reports are delivered on time.
2	Maintain Overall Effectiveness of the IT Financial Management Process	5	Financial Management Tooling Support Level. NGEN toolsets that support financial management activities will facilitate the high level of process maturity. Evaluated as a COBIT maturity process level.
		6	Financial Management Process Maturity.

			NGEN will execute financial management to a high-level of process maturity. Evaluated as a COBIT maturity process level.
		8	Number of Financial Reports/Forecasts Delivered Late. The NGEN financial management process will ensure financial reports are delivered on time.
3	Recapture IT Costs Through Chargeback for Delivery of IT Services	5	Financial Management Tooling Support Level. NGEN toolsets that support financial management activities will facilitate the high level of process maturity. Evaluated as a COBIT maturity process level.
		7	IT Invoicing/Payment Variance. Determine how much of obligated funds were not actually paid out. = Total obligated funds minus Total paid funds.
4	Ensure Customers are Satisfied with Costs and Charges for Services	9	Number of Changes to Charging Algorithms. Changes to algorithms used to formulate payment for IT Services is an indicator of customer satisfaction. If no changes and customers are satisfied, no changes were needed. If no changes and customers are dissatisfied, changes should've been made. If changes were made and customers are still dissatisfied, changes were inadequate or incorrect.

2.4.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Financial System (ERP, etc.)
- Service Knowledge Management System (SKMS)

3 Service Design

Service Design focuses on the activities that take place in order to develop the strategy into a design document which addresses all aspects of the proposed service, as well as the processes intended to support it. Key areas in this volume are: Service Catalog Management, Service Level Management, Capacity Management, Availability Management, Information Security Management, IT Service Continuity Management, and Supplier Management.

3.1 Service Catalog Management

3.1.1 Process Overview

The Service Catalog is the single source of consistent information on all the agreed services and consists of ALL a service providers operational capabilities. The Service Catalog reflects current details, status, interfaces and services in operation or being planned for operations.

The objective of the Service Catalog is to provide and maintain accurate details, status, interfaces and dependencies of all NGEN service that are being transitioned or have been transitioned to the live environment.

3.1.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

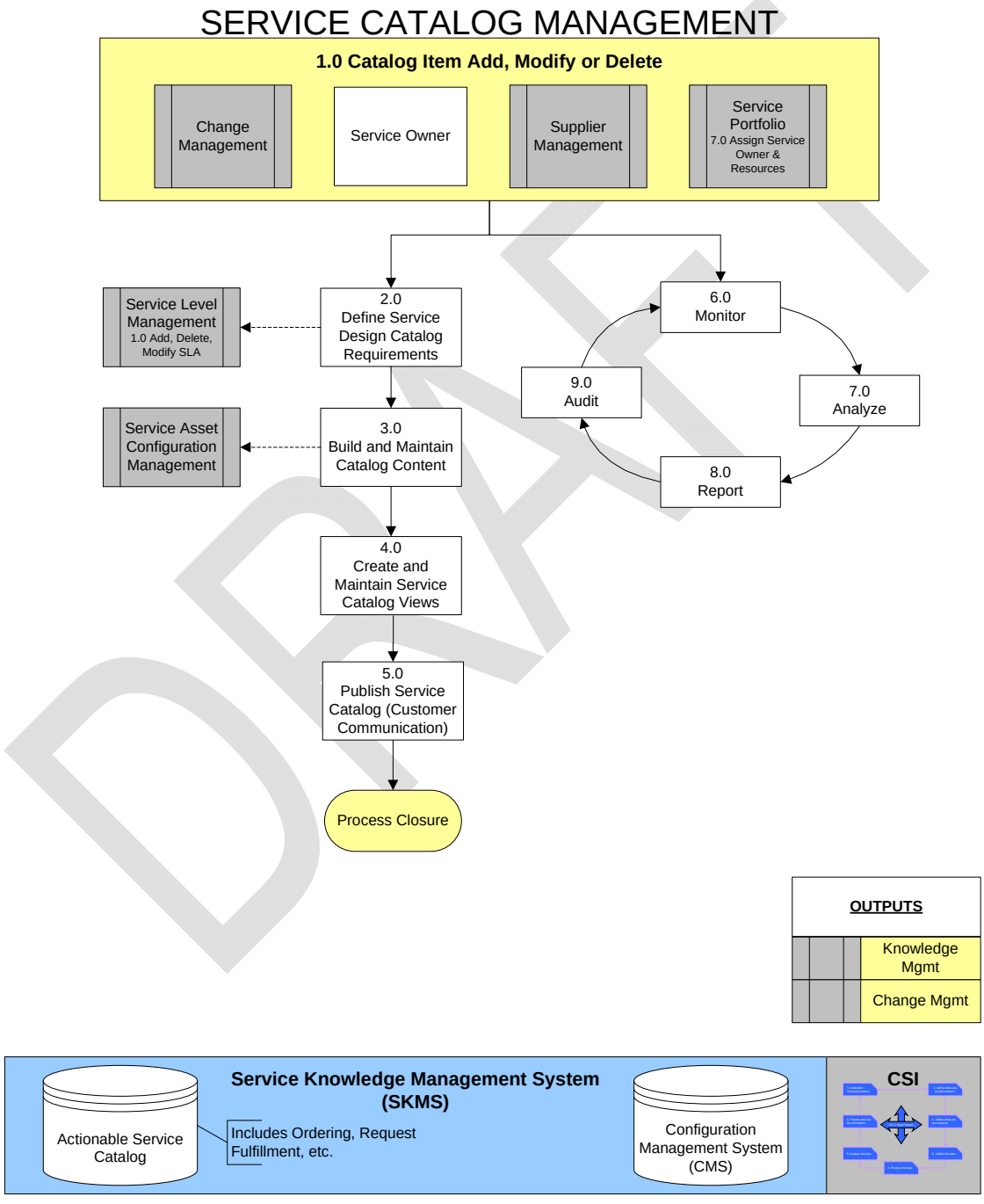


Figure 6 Service Catalog Management Model

3.1.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Catalog Item Add, Modify or Delete	Enter and update service definitions, navigate support, determine view management, identify service selection and transaction tracking, and educate NGEN user on how to use the Service Catalog.
2.0	Define Service Design Catalog Requirements	Collect and analyze Service Catalog Design Requirements, as provided by Service Portfolio Management. Validate requirements with stakeholders for completeness, consistency, and verifiability. Establish the Business Service Catalog comprised of customer views. Views contain details of all NGEN services delivered to the end-user together with relationships to the organizations and processes that rely on NGEN services. Establish the Technical Service Catalog containing details of all IT services delivered to the end-user, together with relationships to the supporting services, shared services, components, and CIs required to support the provision of the service to NGEN.
3.0	Build and Maintain Catalog Content	Determine the scope of Service Catalog content. Develop Service Catalog specifications from requirements already identified. Create and maintain standard templates for service descriptions. Load service descriptions (including standards terms and conditions, available levels of service, etc.) into the Service Catalog. Establish and enforce editing/archiving rules, authorities, and accountability of the content.
4.0	Create and Maintain Service Catalog Views	Define preferred access and navigation patterns by user community and role. Establish search / view/ update schema and mechanisms for use by administrators and end users. Maintain the library of active and inactive searches/views based on utilization. Verify Catalog integrity and performance of all views through testing,

		inspection, simulation, and/or load testing.
5.0	Publish Service Catalog (Customer Communications)	Provide appropriate access mechanisms for customers/users and providers/suppliers to Catalog content. Provide training and support for customers/users and providers/suppliers on the proper use of the Service Catalog. Provide appropriate notifications to the appropriate user community when changes are made to the Catalog (e.g., line items, content, terms and conditions, decommissioning, etc.) Establish and communicate refresh schedules for remote or replicated Catalog versions. Maintain comprehensive version control and coordination across Service Catalog instances. Include development, test, and production environment version control.
6.0	Monitor	Monitor content of the Service Catalog. Produce a Service Catalog that includes the details and current status of every live service provided by the service provider or service being transitioned into the live environment. Include relevant interfaces and dependencies.
7.0	Analyze	Analyze content of the Service Catalog to ensure that the information is salient and up to date. Ensure information is consistent with information in the Service Portfolio and Configuration Management and Knowledge Management systems.
8.0	Report	Produce reports to record metrics regarding the provided services and related dependencies. Update to the Service portfolio; include current status of all services and requirements for each service(s).
9.0	Audit	Periodically audit the Service Catalog Management process to ensure process efficiency.

3.1.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Service Owner
	Own and maintain the Service Catalog.	CI	AR	R	R
	The single NGEN Enterprise Service Catalog shall consist of a Business and Technical Service catalog. • The Business Catalog (Customer view) contains details of all IT Services delivered to the customer together with relationships to the SYSCOM, Offsite Contract Support, Fleet Commands, Operational Units, United States Marine Corps (USMC), COIs, etc. and workflows (approval, financial, provisioning, delivery) that rely on the IT process. (Example: standard service requests, on boarding New Employee, which may include a bundle of services including laptop, email account, blackberry, etc.). • The Technical Catalog (Operational view) contains details of all IT Services delivered to the customer, together with relationships to the supporting services, shared services, components and Configuration Items (CIs) necessary to support the provision of the Service to the Business.	CI	AR	R	R
	Use or interface with the Government	CI	AR	R	R

	(DON) Service Catalog Management Tool to ensure there is a single source of record for all live IT Services.				
	Ensure that all Services are entered in the Service Catalog prior to fielding/provisioning that Service.	CI	AR	R	R
	Provide the Catalog Manager with all necessary information applicable to a service including the following: • Product(s) and Service(s) description • CI and CI relationships (compatibility and dependencies) • Implementation constraints and requirements • Anticipated Availability and Retirement dates • Pricing • Maintenance Schedule (planned or pre-planned unavailability) • User instructions/user guides for utilizing for the Service • Ordering/Request/Delivery Instructions and Service Level Agreements (SLAs)	CI	AR	R	R
	Notify the Government (x) days (service specific requirement) in advance of the "end of life/retirement" for any service.	CI	AR	R	R
	Notify the Government (x) days (service specific requirement) in advance of the "end of life support".	CI	AR	R	R
	Collaborate with the Government Service Catalog Process Manager to: • Maintain accurate and up-to-date information for their Services in the Service Catalog on a daily basis • Identify and implement changes to the process • Identify exceptions and deviations, as well as management of these situations • Provide resource commitment and allocation • Identify and implementing process	CI	AR	R	R

	improvement • Create, analyze and distribute process reports • Resolve issues with items not complying with the process • Escalate issues when needed, as defined in the escalation policy • Notify the participants in the process when standards and procedures are not being followed • Ensure completeness and integrity of information collected to conduct daily operations • Audit the process for compliance with documented procedures.				
	Adhere to the Government's CI data model and naming conventions (see Asset and Configuration Management).	CI	AR	R	R
	Provide the following reports on a weekly basis in a format specified by the Government (the Government will also have system access to generate these reports): • The number of services recorded and managed within the Service Catalog as a percentage of those being delivered and transitioned into the live environment • The number of variances detected between the information contained within the service Catalog and the 'real-world' situation.	CI	AR	R	R

3.1.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Service Planning
- Service Level Management
- Availability Management
- IT Service Continuity Management

- Capacity Management
- Financial Management
- Change Management
- Supplier Management.

Inputs

Consider the inputs to the process:

- Request for Change (RFC)
- Updates to Service Portfolio
- Services needed
- Actual cost
- Map demand patterns and PBA
- Service Information
- Catalog updates
- Catalog
- Service Information.

Outputs

Consider the outputs from the process:

- Service Levels
- KEDB
- Forward Schedule of Change (FSC)
- CI Information
- Service releases.

3.1.6 Roles

The following roles have been identified with the process.

Roles	Description
Service Catalog Process Owner	The strategic role that is accountable for the Process as well as the tactical role that performs cross
Service Catalog Process Manager	The tactical role that performs cross-segment coordination and ensures that the Catalog is accurate and up-to-date and Process requirements outlined below are met.
Service Owner	A role that is accountable for the delivery of a specific IT

	Service.
Service Provider Lead	The operational role that coordinates activities and supervises resources in the performance of Process Activities within their Segment.

3.1.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Maintain an accurate service catalog.	1	Amount of missing information in the service catalog, including all specific customer views.
		2	Amount of incorrect or outdated information in the service catalog, including all specific customer views.
		3	Authorized and timely changes made to service catalog, including all specific customer views. Examples: adding new services, altering existing services, retiring services.
2	Create business user awareness.	4	Proportion of accurate and timely customer notifications on changes to the service catalog.
		5	Proportion of accurate and timely updates to the SKMS.
3	Create staff awareness.	6	Proportion of accurate and timely staff notifications on changes to the service catalog.
		5	Proportion of accurate and timely updates to the SKMS.

3.1.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Actionable Service Catalog
- Configuration Management System
- Knowledge Management System

3.2 Service Level Management

3.2.1 Process Overview

Service Level Management (SLM) is the process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on service levels, and holds regular customer reviews.

The goal for SLM is to maintain and improve IT Service quality, through a constant cycle of agreeing, monitoring and reporting upon IT Service achievements and instigation of actions to eradicate poor service - in line with business or Cost justification. Through these methods, a better relationship between IT and its Customers can be developed.

.

3.2.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

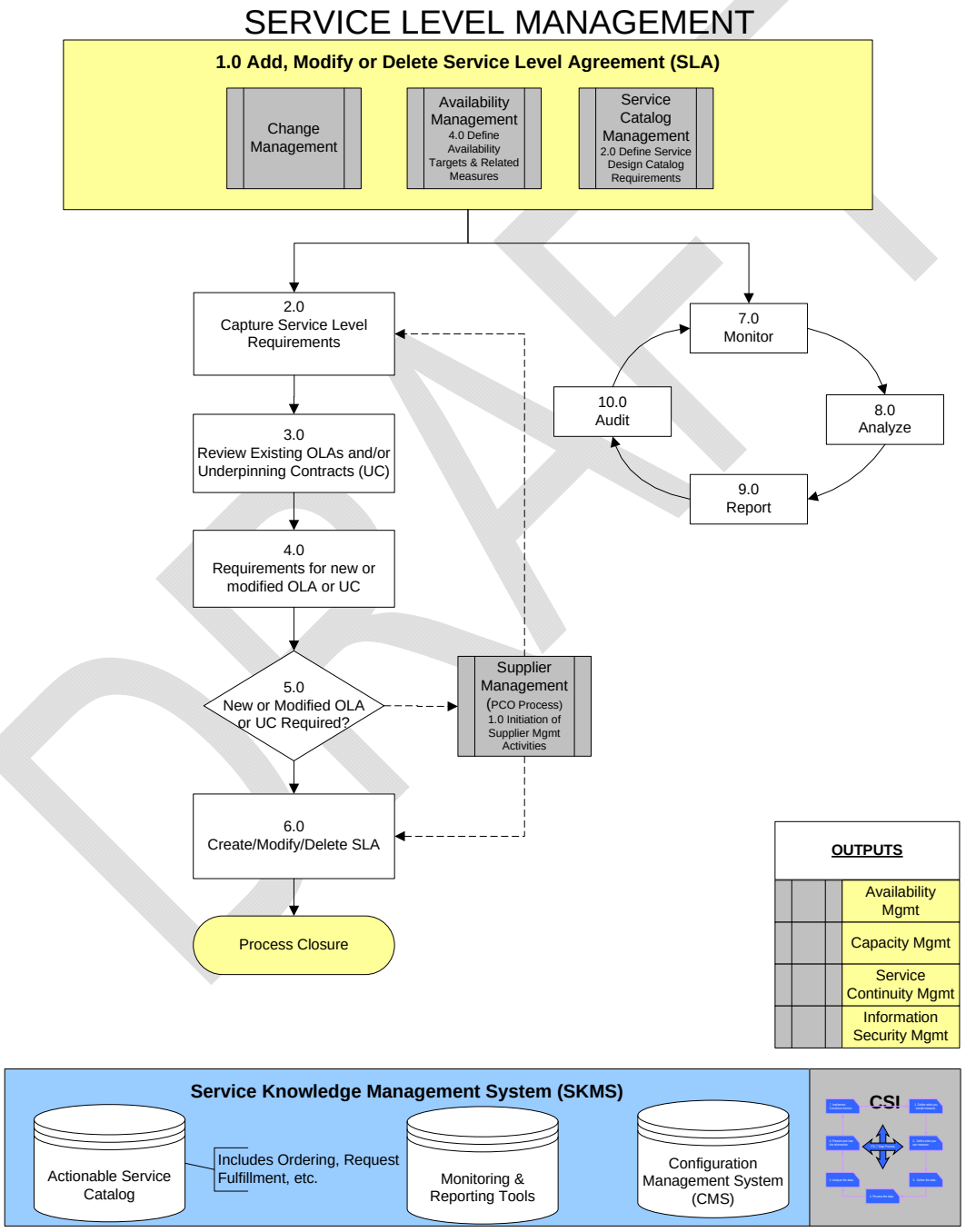


Figure 7 Service Level Management Model

3.2.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Catalog Item Add, Modify or Delete Service Level Agreement	Modification, addition and/or deletion of agreements may occur due to changing needs of NGEN or in response to supplier performance. Define SLAs based on the NGEN Service Catalog and add to agreements managed by the SLM process.
2.0	Capture Service Level Requirements	Identify the necessary requirements needed to deliver the service. (Example: targets for availability, capacity, security, and disaster recovery.)
3.0	Review Existing OLAs and/or Underpinning Contracts (UCs)	Identify dependences, such as existing OLA and UC that may affect the addition, modification or deletion of SLA.
4.0	Requirements for new or modified OLA or UC	Explore the impact of dependencies to the SLA Identify updated requirements for OLA and UC that support live services.
5.0	New or Modified OLA or UC Required?	Determine whether an OLA or UC needs to be created or modified to support the creation, modification or deletion of an SLA. Forward all requests for new OLAs and UCs to Supplier Management (Program Contractor Office (PCO) Process).
6.0	Create/Modify Delete SLA	Create Modify or Delete SLA based on impact to NGEN and suppler performance.
7.0	Monitor	Monitor service performance against established SLAs.
8.0	Analyze	Analyze service performance against established SLAs and business requirements.
9.0	Report	Produce service reports to record level of service achievement. These reports contain details of performance against SLA targets as well as any trends in performance. Breaches of service levels

		will be highlighted prominently.
10.0	Audit	Audit service performance periodically to ensure process efficiency.

3.2.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	The Service Catalog will be the single source of record for all Service Level Agreements (SLAs).

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Delivery Lead
	Use and/or interface with the Government (DON) Service Catalog management system.	CI	AR	R
	Monitor and / or audit the Service Provider's SLA compliance.	CI	AR	R
	Provide a Service Delivery Lead or Team that will be the single point of contact for this Process. This is the operational role that coordinates activities and supervises resources in the performance of Process Activities within their Segment.	CI	AR	R
	Comply with all SLAs provided by the	CI	AR	R

	Government.			
	Provide reports derived from details and frequencies dictated by service design packages. Reports shall ensure measurement activities are value-based. The Government (DON) will work with the Service Provider to determine output for these reports based on what the Government wants to accomplish. The Government (DON) will also have system access to generate these reports.	CI	AR	R
	For LOS 2 and higher level services, report all failures to meet SLAs within (x) hours/days (recommend no more than 24 hours).	CI	AR	R
	Identify and report significant risks to meeting SLAs.	CI	AR	R
	Provide documentary evidence that issues raised at Service level reviews are being followed-up and resolved	CI	AR	R
	Ensue that any changes to the SLAs will adhere to the Change Management Process owned and directed by the Government.	CI	AR	R
	Ensure that service levels will be monitored and reported against targets, showing both current and trend information. The reasons for non-conformance will be reported and reviewed. Actions for improvement identified during this process will be recorded and provide input into a plan for improving the service.	CI	AR	R
	Ensure there shall be clear policies and Processes for: • Percentage of service targets being met • Number and severity of service breaches • Quantitative and qualitative metrics on SLA targets threatened, SLA targets missed and SLA breaches caused by 3rd party support contracts • Percent reduction in SLA breaches	CI	AR	R

	caused by 3rd party support contracts			

3.2.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Demand Management
- Incident Management
- Service Portfolio Management
- Supplier Management
- Service Catalog Management
- Request Fulfillment
- Service Level Management
- Change Management
- Service Knowledge Management System
- Service Desk (function)

Inputs

Consider the inputs to the process:

- RFCs
- SLA, OLA targets
- New Services
- Actual costs
- Impact on future demands
- Creates Service Catalog
- SLA, OLA
- SLA
- SLA, OLA, Service Catalog
- Review process

Outputs

Consider the outputs from the process:

- Cost estimates

- Service Information
- UC
- Catalog updates
- Security policy considerations for service specs
- RFCs for evaluation
- CI Information
- Release notification

3.2.6 Roles

The following roles have been identified with the process.

Roles	Description
SLM Process Owner	The strategic role that is accountable for the Process.
SLM Process Manager	The tactical role that performs cross-segment coordination and ensures that all Service Catalog SLAs are monitored, analyzed and reported on, and changed or modified as required.
Service Delivery Lead	A Service Provider role responsible for monitoring, analyzing and reporting on the Service Delivery performance of each Segment

3.2.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Manage Quality of IT Services In line with NGEN Requirements	1	Overall Customer Satisfaction Rating. NGEN will maintain history and current status of how customers perceive the quality of services being delivered.
		5	Total Service Penalties Paid. Track how much is being paid in service penalties, either by the Government or service providers.
		6	Percent of SLA Targets Adhered to. NGEN will meet SLAs and measure how well it has met the SLA service targets. This attribute

			measures the required improvement of 2010 - 2013 that service levels are monitored and reported against targets, showing both current and trend information. = 1 minus Total number of SLA service targets breached divided by the Total number of SLA service targets.
		8	Service Level Management Tooling Support Level. NGEN will provide adequate tools to manage the SLM processes. COBIT Maturity Model
		9	Service Level Management Process Maturity. NGEN will execute service level management to a high-level of process maturity. Evaluated as a COBIT maturity process level.
2	Manage the Customer/User Interface.	1	Overall Customer Satisfaction Rating. NGEN will maintain history and current status of how customers perceive the quality of services being delivered.
		7	Percent of SLAs without Responsible Service Owners. NGEN will minimize the percentage of delivered services with SLAs that don't have assigned service owners. = 1 Number of SLAs operating without service owners divided by Number of services delivered to customers/business (SLAs).
		8	Service Level Management Tooling Support Level. NGEN will provide adequate tools to manage the SLM processes. COBIT Maturity Model
		9	Service Level Management Process Maturity. NGEN will execute service level management to a high-level of process maturity. Evaluated as a COBIT maturity process level.
3	Deliver IT Services as Agreed to by Customers and NGEN.	2	SLA Coverage Rate. NGEN will have agreement for level of service for all services or service areas. = 1 minus Number of services without SLAs divided by number of services delivered to customers/business.
		3	OLA Coverage Rate. = 1 minus Number of internal services without OLAs divided by number of internal services delivered to customers/business.
		4	Percent of Vendor Services Delivered Without Agreed Service Targets.

		5	Total Service Penalties Paid. Track how much is being paid in service penalties, either by the Government or service providers.
		6	Percent of SLA Targets Adhered to. NGEN will meet SLAs and measure how well it has met the SLA service targets. This attribute measures the required improvement of 2010 - 2013 that service levels are monitored and reported against targets, showing both current and trend information. = 1 minus Total number of SLA service targets breached divided by the Total number of SLA service targets.
4	Provide Services at an Acceptable Cost.	5	Total Service Penalties Paid. Track how much is being paid in service penalties, either by the Government or service providers.

3.2.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- The Incident Ticketing system will monitor and report SLAs for all Incidents
- The Request Fulfillment tool will monitor and track the SLAs for all request tickets
- Event monitoring tools will contribute to SLA reports

3.3 Capacity Management

3.3.1 Process Overview

Capacity Management is the discipline that ensures IT infrastructure is provided at the right time in the right volume at the right price, and ensuring that IT is used in the most efficient manner.

This involves input from many areas of the business to identify what services are (or will be) required, what IT infrastructure is required to support these services, what level of Contingency will be needed, and what the cost of this infrastructure will be.

The objective of Capacity Management is the ability to produce or make the available IT resources that customer, users and the IT department needs to carry out their work efficiently, and to do so in a cost effective way.

The Capacity Management Process ensures cost-justifiable IT capacity always exists in all areas of IT and is matched to the current and future agreed needs of the business, in a timely manner. There are three focus areas of Capacity Management.

- Business Capacity Management – is responsible for ensuring that the impacts of future business requirements for IT services upon IT resources are considered, planned, and implemented in a timely fashion

- Service Capacity Management - the management of the performance of the IT services used by the customers. It is responsible for ensuring that service performance is monitored, measured, and reported; and meets business requirements and agreements
- Component Capacity Management - the management of the performance, utilization, and capacity of individual technical components possessing finite resources.

•

3.3.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

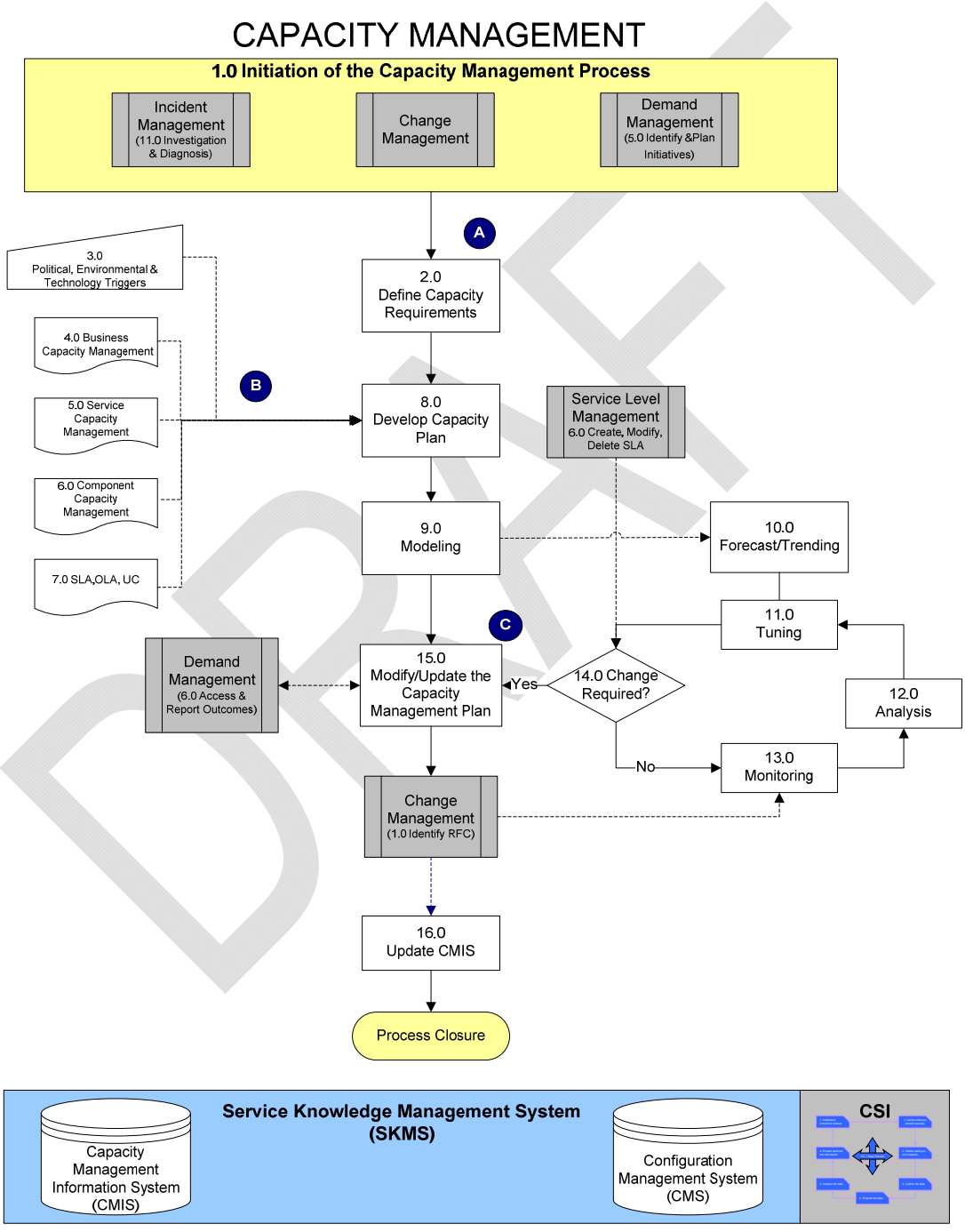


Figure 8 Capacity Management Model

3.3.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of the Capacity Management Process	There are a number of ITIL Processes that are inputs into the Capacity Management Process: • Incident Management – Provide information to help Capacity Management plan for adequate capacity • Change Management – Analyze RFCs requiring a change or impact to capacity • Demand Management – Provide demand actuals and forecasts to produce sizing requirements
2.0	Define Capacity Requirements	Match the capacity of the IT services and infrastructure to the current and future identified needs of NGEN.
3.0	Political, Environmental & Technology Triggers	Evaluate and optimize Capacity based on Availability, Reliability, Maintainability, Serviceability, and Resiliency in light of political, environmental and technology triggers.
4.0	Business Capacity Management	Refine Business Capacity Management requirements.
5.0	Service Capacity Management	Refine Service Capacity Management requirements.
6.0	Component Capacity Management	Refine Component Capacity Management requirements
7.0	SLA, OLA, UC	Refine overall capacity planning needs and requirements based on information contained in SLAs, OLAs and UCs.
8.0	Develop Capacity Plan	Develop a NGEN Capacity Plan which details existing usage of critical IT resources under management. The plan also includes correlation of IT resource usage to IT applications (services) and NGEN usage patterns.

9.0	Modeling	Generate predictive future behavior by representing the system in different capacity scenarios based on peak times in the demand cycle, criticality of workloads, etc.
10.0	Forecast/Trending	Document trends and forecasts responsible for ensuring that the future business requirements of IT Services are considered planned and implemented in a timely fashion.
11.0	Tuning	Tune all components within the IT infrastructure based on NGEN requirements and needs.
12.0	Analysis	Analyze all components within the IT infrastructure to identify utilization trends, bottlenecks, unexpected increases in workload, etc.
13.0	Monitoring	Monitor all components within the IT infrastructure in relation to established threshold and baselines.
14.0	Change Required?	Determines whether the Capacity Management Plan should be updated/modified as a result of the monitoring, analysis and tuning activities.
15.0	Modify/Update the Capacity Management Plan	Modify/Update the NGEN Capacity Plan based on changes authorized by Change Management.
16.0	Update CMIS	Update the Capacity Management Information System with an updates to capacity authorized by Change Management.

3.3.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
A	Identification / Reporting from Multiple Processes to Segment Capacity Manager
B	Define Capacity Requirements / Develop Capacity Plan
C	Process Requirements

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Business Capacity Management Team	Service Capacity Management Team	Component Capacity Management Team	Segment Capacity Management Team
C	Monitor, Analyze and Report on Service Performance	I	AR	R	R	R	R	R
C	Establish Baselines and Profile Use / Demand	CI	AR	R	R	R	R	R
C	Translate Business Capacity requirements into Service and Component Capacity	CI	AR	R	R	R	R	R
C	Define Capacity Thresholds and Alarms	CI	AR	R	R	R	R	R
C	Produce and Maintain Capacity Plan	CI	AR	CI	CI	CI	CI	CI
C	Provide SLA/SLR Recommendations	CI	AR	R	R	R	R	R
C	Provide advice and guidance to all areas of business and IT on performance related issues	CI	AR	R	R	R	R	R
C	Manage Performance and Capacity of Services/Resources by ensuring Service Performance Meets / exceeds all agreed performance targets	CI	AR	R	R	R	R	R

C	Assist with Diagnosis and Performance of capacity related Problems/Incidents	CI	AR	R	R	R	R	R
C	Assess Impact to Capacity Plan from all Changes, Upgrades, RFCs and New Technologies	CI	AR	R	R	R	R	R
C	Assess Performance and Capacity of all Services and Resources	CI	AR	R	R	R	R	R
C	Ensure Proactive measures to improve performance are implemented when cost-justified	CI	AR	R	R	R	R	R
C	Establish methods, procedures and techniques to monitor service capacity, tune service performance and provide adequate capacity	CI	AR	R	R	R	R	R
A	Provide Segment Capacity Management. Representative single point of contact	CI	AR	R	R	R	R	R
B	Provide resources to assist with creation and maintenance of Capacity Plan	CI	AR	R	R	R	R	R
B	Evaluate all RFCs to assess risk and potential impact to Service Capacity	CI	AR	R	R	R	R	R
B	Participate in Problem reviews of capacity-related Incidents to assess risks and potential recurrence of the Incident.	CI	AR	R	R	R	R	R
B	Participate in Review of Capacity related threshold Events (as defined by the DON) to assess risks and potential occurrence of an Incident.	CI	AR	R	R	R	R	R

B	Continuously monitor and analyze the Capacity of the Services provided	CI	AR	R	R	R	R	R
B	Document Capacity trends and forecasts	CI	AR	R	R	R	R	R
B	Ensure trend and forecast information can be viewed by DON on demand	CI	AR	R	R	R	R	R
B	Submit RFC to modify or increase capacity-related services IAW DON's Change Management Process	CI	AR	R	R	R	R	R

3.3.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Service Level Management
- Incident Management
- Problem Management
- Change Management
- Demand Management

Inputs

Consider the inputs to the process:

- Resource forecasting
- Request for Change (RFC)
- Capacity related Incidents
- Performance monitoring
- Workload monitoring
- Demand forecasting
- Modeling and work loading
- Explanations of capacity related Incidents

Outputs

Consider the outputs from the process:

- Capacity Plan
- Forecasts
- Tuning Data
- Service Levels
- Cost estimates

3.3.6 Roles

The following roles have been identified with the process.

Roles	Description
Process Owner	Accountable for ensuring that a process is fit for purpose and will achieve standardization of Capacity Management processes across the NGEN enterprise. The Process Owner's responsibilities include sponsorship, process design and continual process improvements, including process metrics and reports.
Process Manager	A tactical role that is responsible to oversee the daily process activities. This person performs cross-segment coordination of Capacity Management activities. S/he ensures that current and future Capacity requirements for the enterprise are identified and weighed against the infrastructure needs of NGEN balanced against forecasted demand and Service Level Agreements are consistently met.
Business Capacity Management Team	A team of managers who operate under the direction of the Capacity Management Process Manager. These Process Managers oversee activities related to Capacity Management's Business Capacity Management activities. This is the tactical role that performs cross
Service Capacity Management Team	A team of managers who operate under the direction of the Capacity Management Process Manager. These Process Managers oversee activities related to the Business Capacity Management sub
Component Capacity Management Team	A team of managers who operate under the direction of the Capacity Management Process Manager. These Process Managers oversee activities related to Capacity Management's Business Capacity Management sub

Segment Capacity Management Representative	This is the operational role that coordinates activities and supervises resources in the performance of Process activities within a specific Segment. There is only ONE representative (point of contact) for this process within each Segment. Specifically, the Service Provider will have resources that will serve as the single point of contact for the Service Capacity Management and Component Capacity Management sub-Processes.

3.3.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Provide accurate capacity forecasts	3	IT Resource Forecast Accuracy Ratio. Critical to accurately forecast IT resource needs. = 1 minus the Number of missed IT resource forecasts divided by the Number of IT resource forecasts.
		4	IT Service Forecast Accuracy Ratio. NGEN must accurately predict workload volume for services. = 1 minus Number of missed IT service forecasts divided by the Number of IT service forecasts.
		5	IT Requirements Forecast Accuracy Ratio. NGEN must accurately anticipate requirements growth and changes. = 1 minus Number of missed IT requirements forecasts divided by the Number of IT requirements forecasts.
2	Provide services with appropriate capacity to match business needs	6	Number of Incidents Caused by Inadequate Capacity. How many Incidents was the result of inadequate capacity?
		8	Capacity Management Process Maturity Level. NGEN must have an increasing maturity level in processes that manage capacity. Moreover, the processes must encompass all aspects of capacity, including server and application scaling, data storage, facilities to support all aspects of the delivery and support of services, including staging, server rooms, helpdesk operations, etc. Evaluated with regards to COBIT maturity

			model for capacity management.
3	Protect services from capacity related Incidents	6	Number of Incidents Caused by Inadequate Capacity. How many Incidents was the result of inadequate capacity?
4	Demonstrate cost-effectiveness through accurate capacity planning	1	Total Expenses for Unplanned Capacity. Planned costs are normally less expensive than unplanned and ad hoc expenses for a program. Further, accurate planning is informative to the POM decision cycle. NGEN will have accurate records of unplanned capacity costs for HW/SW/network components.
		2	Percent of IT Costs for Unplanned Capacity Expenses. For a program, planned costs are normally less expensive than unplanned and ad hoc expenses. Further, accurate planning is informative to the POM decision cycle. NGEN will have accurate records and determine the percent of actual HW/SW/network costs were for unplanned capacity. = Total expenses for unplanned capacity divided by Total actual IT costs for HW/SW/network.
		7	Capacity Management Tooling Support Maturity Level. How well the current tool set supports capacity management activities. Evaluated with regards to COBIT maturity model for capacity management.

3.3.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- The Service Provider shall create and maintain a Capacity Management Information System (CMIS) that holds all capacity management data.
- The Service Provider will require access to all tools that monitor and report on IT Capacity.

3.4 Availability Management

3.4.1 Process Overview

Availability Management is the process responsible for defining, analyzing, planning, measuring and improving all aspects of the availability of IT services. Availability Management is responsible for ensuring that all IT infrastructure, services and tools, etc. provide cost effective and sustained levels of availability defined by business service level targets.

Key Objectives of Access Management are:

Produce and maintain an appropriate and up-to-date Availability Plan that reflects the current and future needs of the business

Provide advice and guidance to the business on all availability related issues

Assist with the diagnosis and resolution of availability related Incidents and Problems

Assess the impact of changes on the Availability Plan

Ensure plans for improving availability whenever it is cost justifiable

Availability Management is primarily concerned with understanding how IT services support the business and with formulating availability and recovery design criteria to achieve desired service level targets. This process works in partnership with both Service Level Management and Capacity Management to ensure service level targets are known and sufficient capacity exists to meet availability thresholds during normal operational conditions. It also works closely with IT Service Continuity Management to optimize service availability during unplanned outages and major Incidents or disasters.

3.4.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

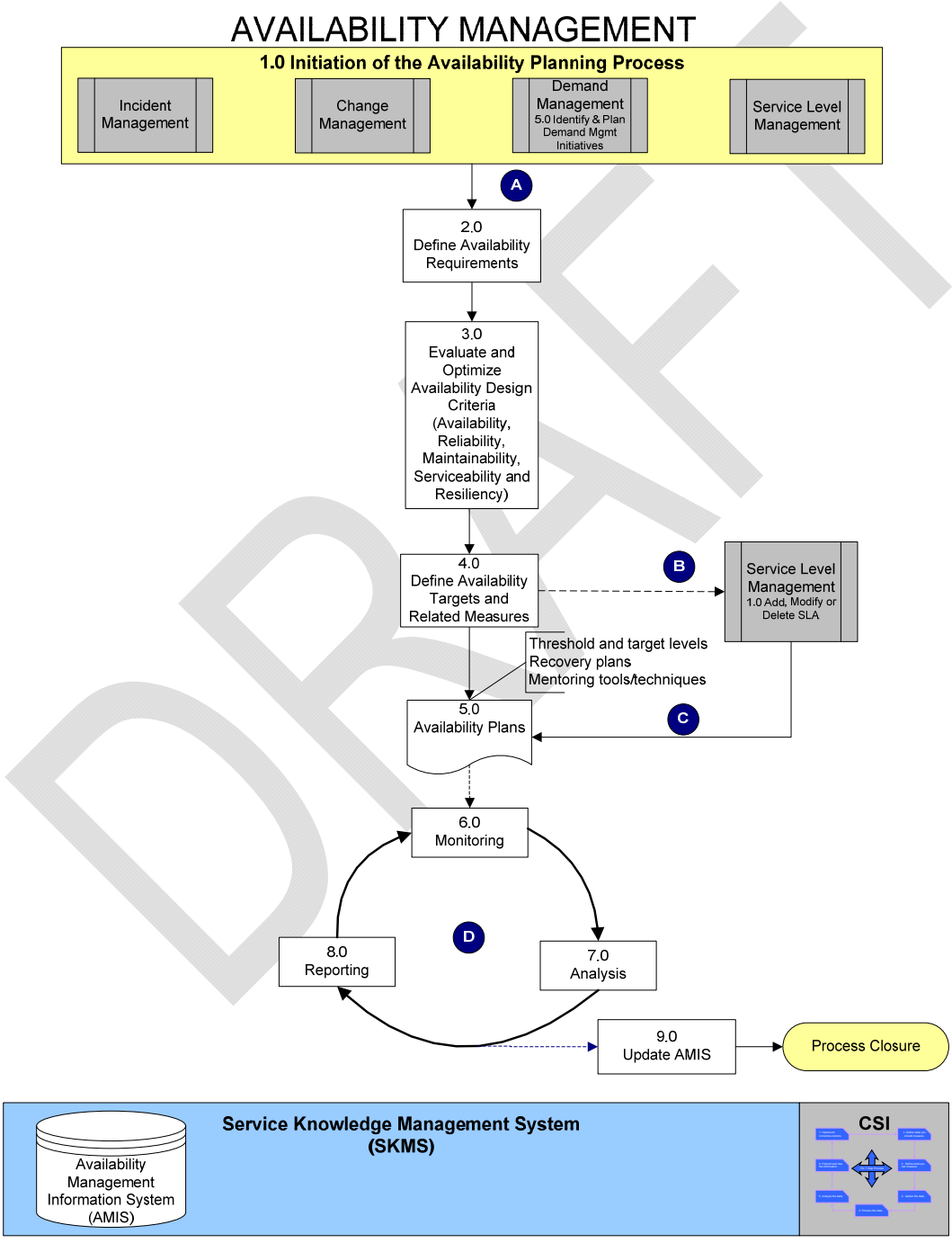


Figure 9 Availability Management Model

3.4.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of the Availability Management Process	Develop IT Strategy and the architectural models, guidelines and a framework for Availability Management
2.0	Define Availability Requirements	Translate NGEN user and IT stakeholder requirements into quantifiable availability terms and conditions and targets, and then into availability-specific requirements that eventually contribute to the Availability Plan.
3.0	Evaluate & Optimize Availability Design Criteria	Evaluate and optimize based on the five factors of Availability (Availability, Reliability, Maintainability, Serviceability, and Resiliency.)
4.0	Define Availability Targets and Related Measures	Provide the following specific measures 1.) Availability, 2.) Reliability and 3.) Maintainability. Verify or ensure measures are agreed to and monitored by Service Level Management.
5.0	Availability Plans (artifact)	Create Availability Plans which summarize resources for availability optimization decisions and commitments for the planning period. Plan includes availability profiles, targets and issues as well as descriptions, historical analyses of achievements with regard to targets summaries, and documented useful lessons learned.
6.0 – 8.0	Monitor, Analyze and Report Availability	Monitor and analyze operational results data and compare with service achievement reporting to identify availability trends and issues. Maintain and improve IT Service quality, through a constant cycle of agreeing, monitoring and reporting IT Service achievements. Instigated actions to eradicate poor service; in line with NGEN or Cost justification.
9.0	Update AMIS	

3.4.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
A	Defining Availability Requirements
B	Validating Availability Targets and Related Measures
C	Reconciling Availability Plans
D	Daily Availability Management Operations

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	Service Availability will be defined, implemented and managed from the end user's perspective of a service.
	When a service is provided by multiple segments, each segment shall manage its own Operating Level Agreements (OLAs)/Underpinning Contracts (UCs)

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes..

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead
	Provide resources to assist with the creation and maintenance (semi-annually) of the NGEN Enterprise Availability Management Plan. This plan will include: • Evaluate all RFCs to assess risks and potential impact to service availability. • Evaluate capacity and demand forecasts to assess risks and potential impact to service	CI	AR	R

	availability. • Participate in post-Incident reviews to assess risks and potential recurrence of the Incident. • Participate in reviews of threshold Events (as defined by the Government) to assess risks and potential occurrence of an Incident. • Participate in an evaluation of the SLAs for its services to ensure they are achievable and measurable. • Participate in the assessment of business impact and risk, provision of resiliency failover and recover mechanism (Service Continuity plan). • Monitor, analyze and report monthly on Availability to the Government (covered by SLA report). • Immediately inform the Government in the event that Availability drops below (x) percent.			
	Provide resources to assist with the diagnosis and resolution of performance and Availability related Problems and Incidents, and report analysis results within (x) days	CI	AR	R
	Provide reports for all services within this segment on a monthly basis for the following: • The Availability of a service, component, or CI to perform its agreed function when required. The percentage of Availability is calculated as: (agreed service time – down time) divided by agreed service time = service availability • Reliability is a measure of how long a service, component, or CI can perform its agreed function without interruption. This will be calculated by (available time in hours – total down time in hours)	CI	AR	R

	divided by number of breaks • Maintainability is a measure of how quickly and effectively a service component or CI can be restored to normal working after a failure. Calculated as (total downtime in hours divided by number of service breaks) ITSM COE has made the assumption that the SME teams for each segment will consult specific KPPs, KSAs and KPIs for the services within this segment to tailor these report metrics.			

3.4.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

- This process has a key relationship or dependency with the following ITSM processes:
- Service Level Management
- Capacity Management
- Incident Management
- Problem Management
- IT Service Continuity Management

Inputs

Consider the inputs to the process:

- Business Availability Requirements
- Service Level Agreements & Service Level Achievements
- Business Impact Assessments
- Availability, Reliability and Maintainability Requirements
- Incident and Problem Data
- Configuration and Monitoring Data

Outputs

Consider the outputs from the process:

- Availability and Recovery Criteria
- Availability Techniques
- Targets for Availability, Reliability and Maintainability

- Availability Reporting
- Monitoring Requirements
- Availability Plan

3.4.6 Roles

The following roles have been identified with the process.

Roles	Description
Availability Process Owner	This is the strategic role that is accountable for the Process.
Availability Process Manager	This is the tactical role that performs cross-segment coordination and ensures that the Availability of all Services consistently meet SLAs.

3.4.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Demonstrate Cost-Effectiveness Through Effective Availability Planning	1	Total Unplanned Expenses Related to Availability. NGEN will limit unplanned expenses. The unplanned-cost dollars spent maintaining needed availability must approach zero.
		4	Availability Management Tooling Support Level. How well does the current toolset support availability management activities?
2	Provide Services with Appropriate Availability to Match Business Need	2	Availability Resilience Index. NGEN will ensure that the necessary resources are expended on continuity of operations and no more than what is necessary. It will determine how resilient the infrastructure is at protecting essential services. = 1 minus the Total number of customer impacting Incidents divided by the Number of Incidents.
		3	Average Service Reliability Index. NGEN will provide highly reliable services and will measure the reliability of the services that are delivered. = 1 minus the Total unavailable minutes for all services delivered divided by the Total available minutes for all services

			delivered.
		5	Availability Management Process Maturity Level. NGEN will have highly mature processes to manage the availability of services. = The COBIT maturity model for availability management.
		6	Average Internal Supplier Service Reliability Index. NGEN must have current status and historical record of the reliability of internal suppliers supporting our NGEN services. = 1 minus Number of internal supplier targets missed divided by the total number of service targets from internal suppliers.
		7	Average Vendor Supplier Service Reliability Index. NGEN must have current status and historical record of the reliability of vendor suppliers supporting our NGEN services. = 1 minus Number of vendor supplier targets missed divided by the total number of service targets from vendor suppliers.
		8	Security Vulnerability Index. NGEN must have current status and historical records of vulnerability to security threats. = the Number of security related Incidents divided by Total number of Incidents.
		9	Serviceability Index. All of the NGEN infrastructure must have an assigned vendor under contract to support. There must be no elements of the infrastructure without a supporting vendor. = 1 minus Number of HW/SW/networking CIs not supported by vendors divided by the Number of HW/SW/networking CIs.
		10	Availability Risk Index. NGEN will deliver services with associated plans for the availability of the service. = the Number of services not covered by an active availability plan divided by the Number of services in the Service Catalog.
3	Continually Improve Availability of Delivered Services	11	Continuous Availability Improvement Index. NGEN must proactively seek to improve service availability. = 1 minus Number of services without availability review in last three months divided by the Number of services in the Service Catalog.

3.4.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

Availability Management Information System (AMIS)

Configuration Management System (CMS)

Service Knowledge Management System (SKMS)

3.5 Information Security Management

3.5.1 Process Overview

Information Security Management (ISM) seeks to ensure that information security is effectively managed in all service and service management activities relate to the confidentiality, integrity and availability of data, as well as the security of hardware and software components, documentation and procedures.

A basic concept of the Security Management is Information Security or Information Assurance (IA). ITIL seeks to ensure that effective information security measures are taken at strategic, tactical, and operational levels. Information security is considered an iterative process that must be controlled, planned, implemented, evaluated, and maintained.

A computer security event is any observable occurrence in a system or network. Events include, for example, a user connecting to a file share, a server receiving a request for a Web page, a user ending sending electronic mail (e-mail), and a firewall blocking a connection attempt. A reportable event is an event with a potentially negative consequence, such as unauthorized system access, system crash, network packet flood, unauthorized use of system privileges, defacement of a web page, or the execution of malicious code that destroys data. All categories of Incidents (see Incident Management) are considered to be NGEN reportable events.

3.5.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

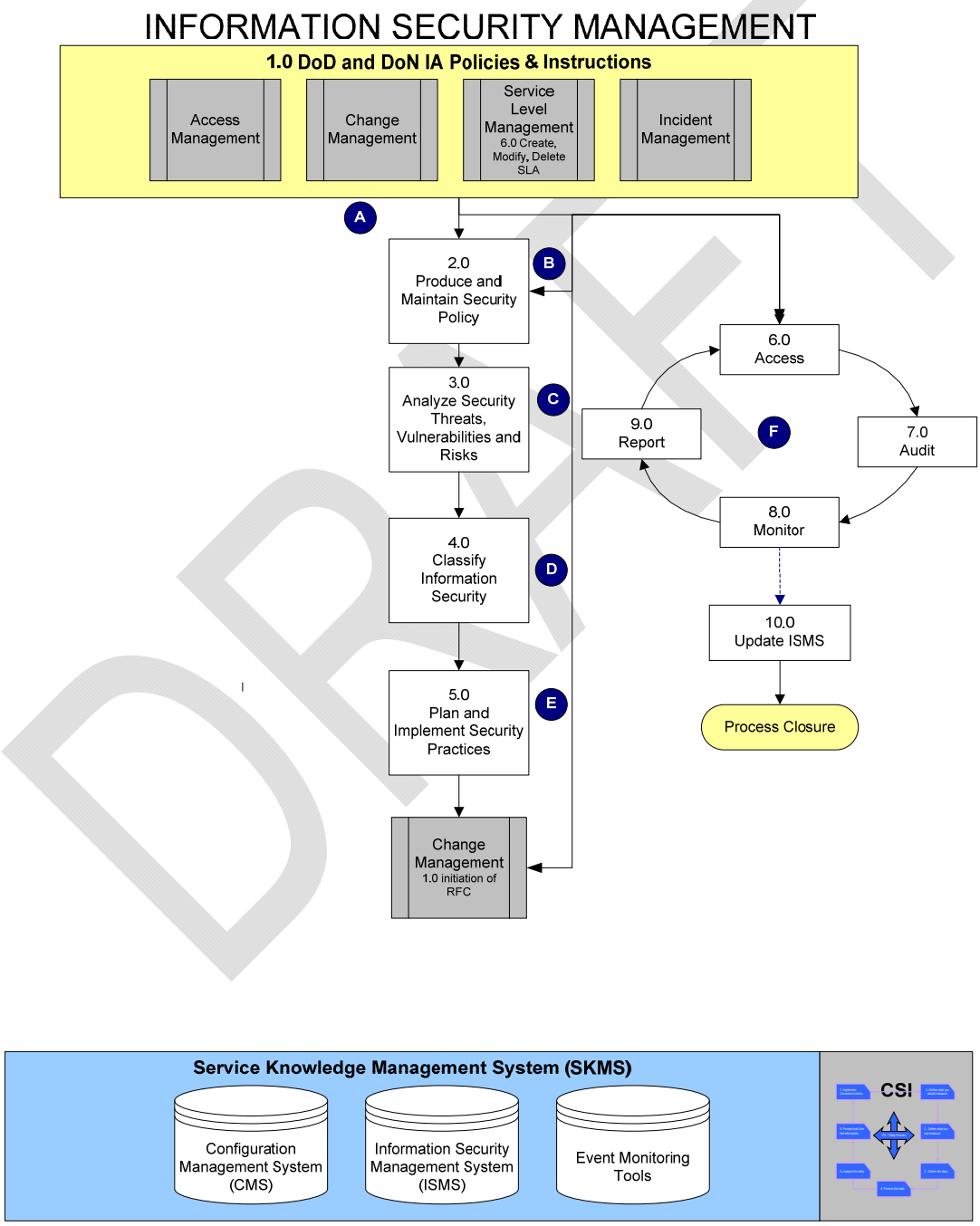


Figure 10 Information Security Management Model

3.5.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	DoD and DON IA Policies & Instructions	Identify DoD and DON Information Assurance Policies and Instructions to ascertain statutory requirements of the NGEN Security Management policy.
2.0	Produce and Maintain Security Policy	Create the overall statement of the aims and objectives for the security to be established and operated in relation to NGEN services and resources.
3.0	Analyze Security Threats, Vulnerabilities, and Risks	Identify security threats, determining risks and vulnerabilities that affect or can affect the IT organization. Recommend mitigating changes based on this analysis.
4.0	Classify Information Security	Develop a security classification scheme for information assets by examining your inventory, identifying the required level of security for each category.
5.0	Plan and Implement Security Practices	Establish a Security Plan defining and creating an appropriate security infrastructure and procedures.
6.0	Access	Establish prescribed security controls and procedures throughout NGEN Apply mechanisms so as to involve the full range of education and training, installing new systems and testing to ensure that security controls and procedures work properly
7.0	Audit	Carry out audits.
8.0	Monitor	Actuate and monitor the full range of security measures and capabilities, responding to service or resource access authorization requests in addition to noting security violations and initiating Incidents when necessary (real-time intrusion detection sensing and immediate responses are both important)

9.0	Report	Create historic reports based on the monitoring data.
10.0	Update ISMS	Update Information Security Management System (ISMS). Review security controls and mechanisms, determining whether they appropriately and effectively implement security policies and procedures as described in the Security Plan.

3.5.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Enterprise ISM Team
	Ensure Service personnel /subs have the correct level of access (CAC access), physical access, account rights and clearance(s) to perform the required services.	ACI	R	R	R
	Conform to the Government's IA security policies, processes and	ACI	R	R	R

	procedures.				
	Provide a weekly detailed and summary report to the Government that contains the following information: • Percent decrease in security breaches reported to the Service Desk • Percent decrease in the impact of security breaches and Incidents • Percent increase in SLA conformance to security clauses • Number of risks and vulnerabilities identified that could impact the Service Provider's provision of services.	ACI	R	R	R
	Provide resources to assist the Government with regular and periodic auditing of its IT Security Management performance.	ACI	R	R	R
	Actively monitor services to ensure compliance with the Government's IA requirements.	ACI	R	R	R
	Continuously analyze the risks and vulnerabilities of Services and report these results to the Government.	ACI	R	R	R
	Coordinate with the Government to provide advice and information to all other dependant or related service providers on security-related issues.	ACI	R	R	R
	Provide resources to assist in the resolution of a security Incident related to its Services.	ACI	R	R	R
	Provide regular and timely updates on changes to Government security policies. The Service Provider shall analyze the impact to its services and implement changes (working through the Government's Change Management process) necessary to ensure the compliance of its services.	ACI	R	R	R

3.5.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Incident Management & Service Desk
- Problem Management
- Change Management
- Service Level Management
- Knowledge Management
- Availability Management
- Release Management
- Configuration Management
- IT Service Continuity Management
- Access Management
- Event Management

Inputs

Consider the inputs to the process:

- DoD and DON Information Assurance Policies and Instructions
- Security Plan including access security
- SLA and Contracts
- RFC
- Security Incident

Outputs

Consider the outputs from the process:

- Updated Information Security Management System (ISMS)
- Updated Configuration Management System (CMS)
- Risk and security reports

3.5.6 Roles

The following roles have been identified with the process.

Roles	Description

ISM Owner (Process Owner)	The Process Owner of the Information Security Management Process s the strategic role that is accountable for the Process.
ISM Manager (Process Manager)	The Process Manager of the IT Service Continuity Management Process is the tactical role that is responsible for cross-segment coordination.
Enterprise ISM Team	The Enterprise IT Information Security Management team (Government organization which is to be determined. Example: NetOps) will be the Process Manager of the Information Security Management Process. This is the tactical role that performs cross-segment coordination and ensures overall compliance with Information Assurance (IA) security policies, processes and procedures.
Segment ISM Lead (Service Provider Lead)	The Service Provider shall have a Segment Information Security Management Lead that shall be the single point of contact for the Information Security Management Process. This is the operational role that coordinates activities and supervises resources in the performance of process activities within their Segment. There is only ONE Lead for each Process within each Segment.

3.5.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Manage the confidentiality, integrity and availability of IT Services	1	Number of security Incidents, caused by internal security failures
		2	Number of security Incidents, caused by external security failures
		3	Number of security audit and testing failures
2	Proactively Addressing Security Improvements Where Needed	4	Number of Security Improvement Initiatives in place
		5	Number of Security Improvement Initiatives completed on time
		6	Number of Security Incidents related to non-

			current security maintenance

3.5.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Event monitoring and system evaluations tools required to fulfill the process requirements.

3.6 IT Service Continuity Management

3.6.1 Process Overview

This Process provides support for the overall Business Continuity Management Process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, Technical Support, and Service Desk) can be resumed within required and agreed business timescales.

NGEN must perform a Business Continuity Needs Evaluation and produce a detailed Business Continuity Strategy that provides the requirements for the IT Service Continuity Strategy and Plan. Note that the requirements and design of each service packages affect the needs for continuity.

IT Service Continuity Management (ITSCM) is about both reactive and proactive measures that reduce the risk of a disaster in the first instance. While continuity management is regarded as the recovery of the IT infrastructure used to deliver IT Services, many businesses these days practice the much further reaching process of Business Continuity Planning (BCP), to ensure the whole end-to-end business process can continue should a serious Incident occur.

To be successful, continuity management can involve conducting a Business Impact Analysis (BIA) to prioritize the businesses to be recovered, perform a Risk Assessment for each of the IT Services to identify the assets, threats, vulnerabilities and countermeasures, produce a Contingency Plan, and test, review and revise the plan on a regular basis.

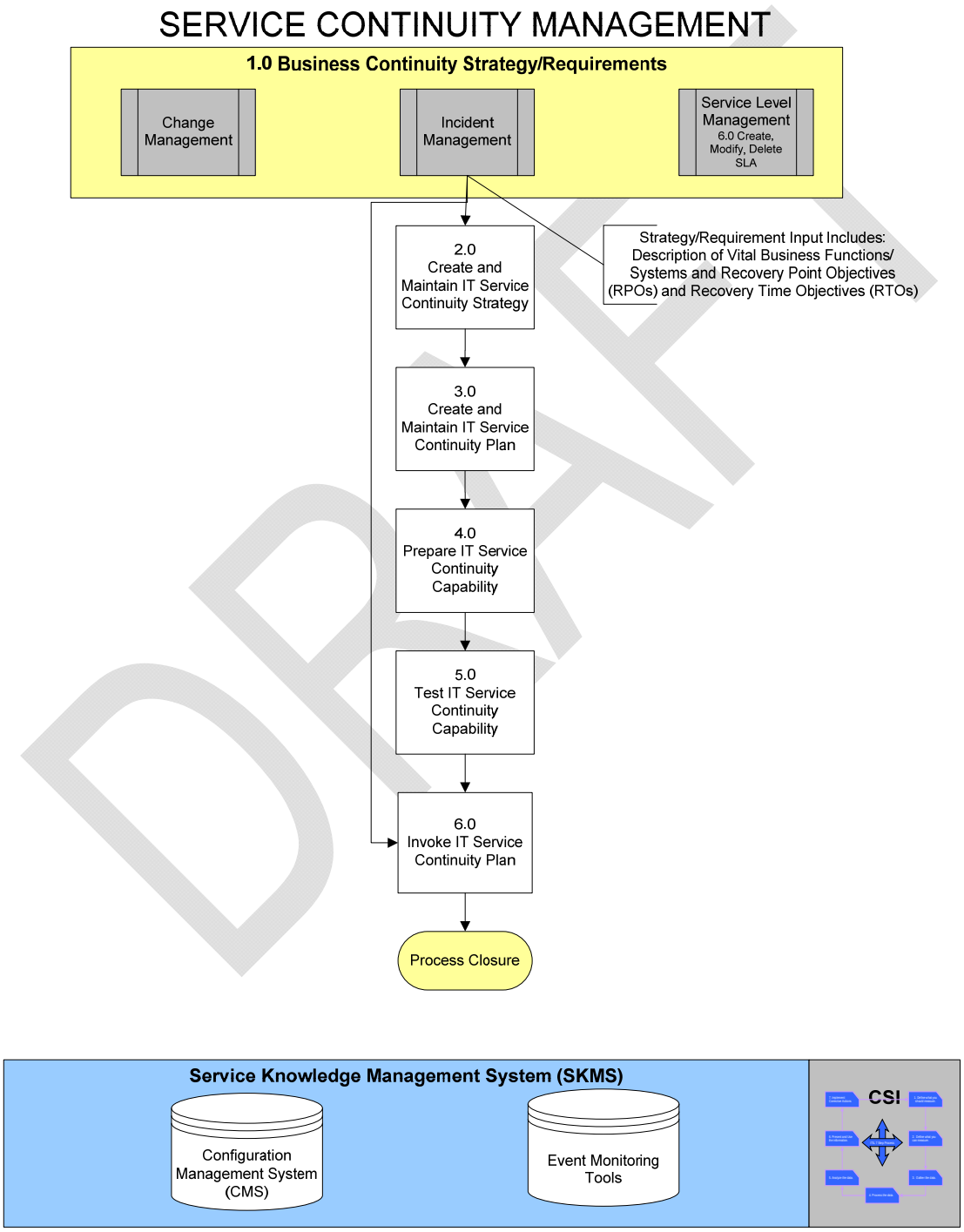
The benefits include minimizing disruption in IT services following a major interruption or disaster and minimizing costs associated with recovery plans through proper proactive planning and testing.

To manage risks that could seriously impact IT services. ITSCM ensures that the IT service provider can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support Business Continuity Management.

3.6.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>



3.6.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Business Continuity Strategy/Requirements	Identify Business Continuity Strategy and Requirements from: Change Management, Incident Management, Problem Management, and/or Service Level Management. Analyze impact of potential loss, disruption or degradation of critical NGEN services.
2.0	Create and Maintain IT Service Continuity Strategy	Identify risk reduction and mitigation measures for critical NGEN services and establish recovery options for service loss, disruption or degradation.
3.0	Create and Maintain IT Service Continuity Plan	Identify the workforce resources, processes and tools needed to restore service and implement successful invocation of the IT Service Continuity Plan. Periodically capture changes to critical NGEN services and supporting infrastructure to update the NGEN Service Continuity Plan.
4.0	Prepare IT Service Continuity Capability	Ensure that the NGEN Service Continuity Plan is tested periodically and that these drills result in restored services at predetermined levels within a predetermined timeframes. Ensure the NGEN Service Continuity Plan passes audit requirements and validate the NGEN Service Continuity Plan processes in light of test results.
5.0	Test IT Service Continuity Capability	Test the NGEN Service Continuity Plan on a planned and ad hoc basis. Capture test results, lessons learned and adjust workforce resources, processes and tools accordingly to optimize restoration of service activities.
6.0	Invoke IT Service Continuity Plan	Implement the NGEN Service Continuity Plan in response to predetermined criteria. Maintain business operations and ensure controlled restoration to normal service.

3.6.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service

Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Enterprise ITSCM Team
	Support the Government in the formulation of Availability and Service Continuity plans that are developed and reviewed at least semi-annually to ensure that requirements are met as agreed in all circumstances from normal through to a major loss of service. Maintain plans to ensure that they reflect agreed changes required.	ACI	R	R	R
	Retest its service continuity plans at every major change to its Services or as directed by the Government.	ACI	R	R	R
	Notify the Government in the event of a service continuity test failure, and formulate and enact appropriate corrective and preventative action plans to address deficiencies in coordination with the Government.	ACI	R	R	R
	Conduct a continuity test for each Service. The mean time between continuity tests must be no greater than 60 days/ This is intended to fulfill the	ACI	R	R	R

	Periodicity Testing requirement from the NGEN requirements document (Table 6.9.8a Appendix VV). Note – Provide one or more continuity reports and these reporting requirements shall be based on the Service Design Package for each Service.				
	In the event the Government's IT Service continuity plan is invoked, provide resources necessary to ensure the required continuity of their services.	ACI	R	R	R
	Provide resources to assist the Government with regular and periodic (at least semi-annually) testing of its IT Service Continuity plan(s).	ACI	R	R	R
	Test no less than 95% of the services it provides that require continuity testing. This is intended to fulfill the Testing Completeness Ratio from the NGEN requirements document (Table 6.9.8a Appendix VV).	ACI	R	R	R
	The Service Provider shall demonstrate the ability to rapidly and completely restore 95% to 99% of its services to the state immediately before the loss of service. This is intended to fulfill the Recovery Confidence Rate from the NGEN requirements document (Table 6.9.8a Appendix VV).	ACI	R	R	R
	The Service Provider shall provide resources to assist the Government with regular and periodic auditing of its IT Service Continuity plan(s).	ACI	R	R	R
	Provide resources to assist with the creation and maintenance (semi-annually) of the NGEN Enterprise IT Service Continuity Plan	ACI	R	R	R
	Evaluate all RFCs to assess risks and potential impact to its service continuity plans.	ACI	R	R	R
	Participate in post-Incident reviews to assess risks and potential recurrence of the Incident.	ACI	R	R	R

	Participate in the assessment of business impact and risk, provision of resiliency failover and recover mechanism (Service Continuity plan).	ACI	R	R	R
	Conform to the Government's Change Management process for implementing any Change related to the Continuity of its services (standard changes will be defined to accommodate day-to-day tuning activities).	ACI	R	R	R
	Coordinate with the Government to provide advice and information to all other dependant or related service providers on continuity and recovery-related issues.	ACI	R	R	R

3.6.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Service Level Management
- Availability Management
- Configuration Management
- Capacity Management
- Change Management
- Service Desk
- Incident Management
- Service Validation
- Event management
- Problem Management
- Access Management

Inputs

Consider the inputs to the process:

- Service Requirements
- ITSCM Plan
- RFC

- Security Policy
- Major Incident
- SLA

Outputs

Consider the outputs from the process:

- Updated CMS
- Updated ITSCM Plan

3.6.6 Roles

The following roles have been identified with the process.

Roles	Description
ITSCM Owner (Process Owner)	The Process Owner of the IT Service Continuity Management Process is the strategic role that is accountable for the Information Security Management Process.
ITSCM Manager (Process Manager)	The Process Manager of the IT Service Continuity Management Process is the tactical role that is responsible for cross-segment coordination.
Enterprise ITSCM Team	The Enterprise IT Service Continuity Management team (Government organization which is to be determined. Example: NetOps) will be the Process Manager of the Information Security Management Process. This is the tactical role that performs cross-segment coordination and ensures overall compliance with Information Assurance (IA) security policies, processes and procedures.
Segment ITSCM Lead (Service Provider Lead)	The Service Provider shall have a Segment IT Service Continuity Management Lead or Team that shall be the single point of contact for the Information Security Management Process. This is the operational role that coordinates activities and supervises resources in the performance of process activities within their Segment. There is only ONE Lead for each Process within each Segment.

3.6.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The

CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Ensure all Required Services can be Recovered from Major Disruptions	1	ITSCM Coverage Ratio. NGEN will prepare service continuity plans for all delivered services. = Number of services covered by IT service continuity plans divided by the Number of services in Service Catalog
		8	ITSCM Process Maturity. NGEN will execute IT service continuity processes to a high level of maturity based on the descriptions of maturity in the COBIT maturity model.
		12	ITSCM Support Service Coverage Ratio. NGEN will maintain the necessary and appropriate agreements with recovery support suppliers. = 1 minus the (P) number of required internal support services without an OLA plus the (Q) number of required external support services without formal agreements divided by the (O) total number of services needed to support IT service continuity plans, 1 - ((P+Q)/O).
2	Recover Services from Major Disruptions within Expected Timeframes	2	Number of Service Continuity Plan Audit Failures. NGEN will seek to minimize service continuity failures. NGEN will need to maintain accurate records for future planning and contractor incentives of the continuity planning failures found during audits.
		5	Testing Completeness Ratio. NGEN will test the continuity for all services delivered. = Number of IT services tested for service continuity divided by the Total number of services in the Service Catalog.
		8	ITSCM Process Maturity. NGEN will execute IT service continuity processes to a high level of maturity based on the descriptions of maturity in the COBIT maturity model.
		9	IT Service Continuity Recovery Confidence Rate. NGEN will recover services rapidly and completely to the state as immediately before the loss of service. = 1 minus the number of services with test failures divided by the total number of services in the Service Catalog.
		10	Number of Continuity Issues Logged Against Service Continuity Plans. NGEN IT service

			continuity plans will be aligned with the DON business continuity plans and operational command continuity plans. Measured according to COBIT maturity model guidelines.
		12	ITSCM Support Service Coverage Ratio. NGEN will maintain the necessary and appropriate agreements with recovery support suppliers. = 1 minus the (P) number of required internal support services without an OLA plus the (Q) number of required external support services without formal agreements divided by the (O) total number of services needed to support IT service continuity plans, 1 - ((P+Q)/O).
3	Maintain Viability of IT Service Continuity Plans	3	Mean Time Between Continuity Tests for Each Service (Months). NGEN will need to verify service continuity plans by frequent testing of those plans.
		8	ITSCM Process Maturity. NGEN will execute IT service continuity processes to a high level of maturity based on the descriptions of maturity in the COBIT maturity model.
		10	Number of Continuity Issues Logged Against Service Continuity Plans. NGEN IT service continuity plans will be aligned with the DON business continuity plans and operational command continuity plans. Measured according to COBIT maturity model guidelines.
		11	Mean Time Between Continuity Plan Audits for Each Service (Months). The NGEN will frequently and periodically audit IT service continuity plans for each service in relation to the IT infrastructure.
4	Provide Service Continuity at Acceptable Costs	4	ITSCM Labor Utilization. NGEN will plan for and expend the labor resources necessary to maintain the user's required availability of services and continuity of services. = Total labor hours used for IT service continuity activities divided by the Total labor hours planned for IT service continuity activities.
		6	ITSCM Cost Rate. NGEN will accurately plan IT service continuity costs. = 1 minus Total unplanned costs for IT service continuity activities divided by the total planned costs for

			IT service continuity activities.
		7	ITSCM Tooling Support Maturity. NGEN tools that support service continuity will be measured according to the COBIT maturity model and achieve and maintain a high level of maturity.

3.6.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Service Desk
- Incident Management System
- CMS

3.7 Supplier Management

3.7.1 Process Overview

The Supplier Management Process ensures that suppliers and the services they provide are managed to support IT service targets and business expectations. The purpose of this Process is to obtain value for money from suppliers and to ensure that suppliers perform to the targets contained within their contracts and agreements, while conforming to all of the terms and conditions.

The objective of Supplier Management is to ensure that all contracts with suppliers support the needs of the DON, and that all suppliers meet their contractual commitments.

Supplier Management ensures that external services and configuration items, which are necessary for the service delivery, are available as requested and as agreed at the service level.

Supplier Management is responsible for the following:

- Consolidating requirements for external services and supplies, scanning the market for providers, negotiating with a chosen supplier, and for the contracting and monitoring of external services and service providers.
- Management of supplier relationships and supplier performance are additional tasks.
- Establishing and updating the basic supplier framework, which is Supplier Strategy and Supplier Policies.

Supplier Management is triggered from the Service Portfolio Management Process whenever a new supplier is necessary.

3.7.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

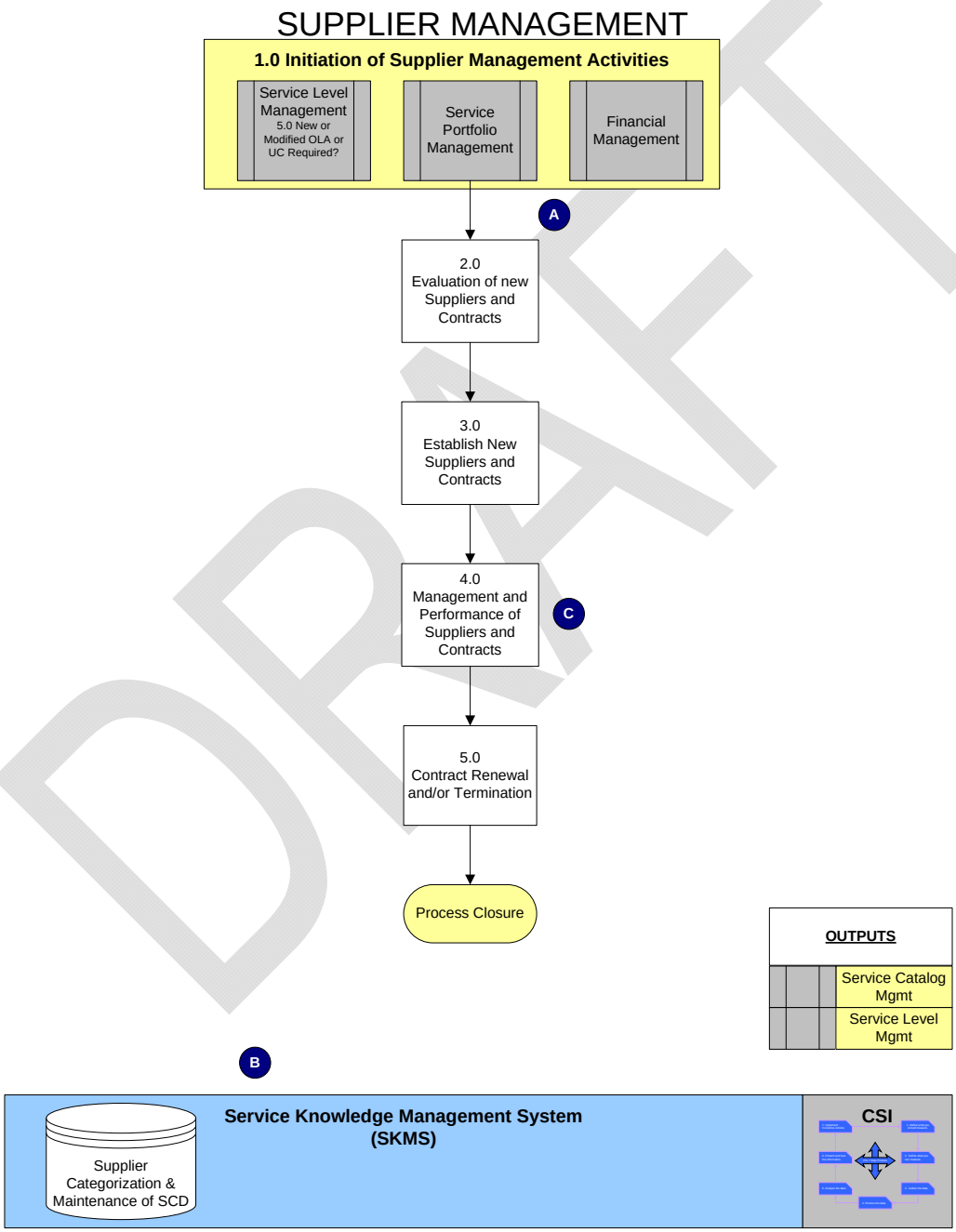


Figure 11 Supplier Management Model

3.7.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of Supplier Management Activities	Aggregate inputs from Service Level Management, Service Portfolio Management and Financial Management to establish the NGEN Supplier Management Strategy.
2.0	Evaluation of new Supplier and Contracts	Evaluate Supplier candidates according to predefined criteria based on acquisition strategy/approach, strategic alignment, Process integration, information flow, performance expectations, budgetary constraints , etc.
3.0	Establish New Suppliers and Contracts	Define scope of Supplier relationship and optimize terms and conditions. Establish Service Level Agreements (SLA), Operational Level Agreements (OLA) and UCs.
4.0	Management and Performance of Suppliers and Contracts	Identify areas of the overall Process that require improvement such as: optimizing the design and interfaces of the Process and activity steps, evaluating possible areas for automation, and updating Supplier Management roles and responsibilities
5.0	Contract Renewal and/or Termination	Examine Supplier based on compliance, performance and service level attainment according to the agreed contracts. This information will be reviewed, the relationship to the suppliers will be evaluated, and the compliance of Suppliers will be analyzed to determine whether to renew or terminate a contract.

3.7.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
A	Supplier Management is the link between the Service Provider and Financial Management.
B	Monitoring, Extracting and Acting on Supplier related data extracted from the SKSM and disseminating Supplier updates and status back into the SKSM system.
C	Supplier Management Representative (Contract Manager 4.0), the single point of contact for this Process.

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	The Supplier Management Process Owner is the strategic role that is accountable for the Process.
	The Supplier Management Process Manager is the tactical role that performs cross Segment coordination.
	The requirements, scope, level of service, and communication processes to be provided by the supplier(s) shall be documented in SLAs or other documents and agreed by all parties.
	There will be one or more Supplier Managers who are responsible for managing customer satisfaction and the whole business relationship Process.
	There shall be a complaints Process. The definition of a formal service complaint shall be agreed with the NGEN user community. All formal service complaints shall be recorded by the service provider, investigated, acted upon, reported, and formally closed. Where a complaint is not resolved through the normal channels, escalation shall be available to the customer.
	The service provider and customer shall attend a service review to discuss any changes to the service scope, SLA, contract (if present), or the business needs at least annually and shall hold interim meetings at agreed intervals to discuss performance, achievements, issues, and action plans. These meetings shall be documented. Other stakeholders in the service may also be invited to the meetings.
	The interfaces between Processes used by each party shall be documented and agreed.
	A Process shall exist to deal with contractual disputes.
	A Process shall be in place to deal with the expected end of service, early end of the

	service or transfer of service to another party.
	The Supplier Management Process Owner is the strategic role that is accountable for the Process.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Supplier Management Team
	Provide a Supplier Management representative (Contract Manager) that will be the single point of contact for this Process. This is the operational role that coordinates activities and supervises resources in the performance of Process activities within their Segment.	CI	AR	R	R
	Use or interface with the DON's Supplier Management Tool (Supplier Contract Database) to ensure there is a single source of record for all supplier related information.	CI	AR	R	R
	Has a documented Supplier Management Processes and names a contract manager responsible for each service.	CI	AR	R	R
	PCO is responsible for negotiating new contracts or modifications to existing contracts.	CI	AR	R	R
	Actively manages the supplier portfolio of services by reviewing, maintaining and optimizing compliance with the NGEN SLAs and other contractual agreements.	CI	AR	R	R
	Negotiate new contracts.	CI	AR	R	R
	Evaluate suppliers and provide alternative options for sourcing services.	CI	AR	R	R
	Perform contract renewal and	CI	AR	R	R

	terminations activities.				
	Create and manage the risk assessment plan related to NGEN IT Service Providers.	CI	AR	R	R
	Identify and document the stakeholders and customers of the services.	CI	AR	R	R
	Changes to the contract(s), if present, and SLA(s) shall follow from these meetings as appropriate. These changes shall be subject to the Change Management Process.	CI	AR	R	R
	Remain aware of business needs and major changes in order to prepare to respond to these needs.	CI	AR	R	R
	SLAs with the suppliers shall be aligned with the SLA(s) with the business.	CI	AR	R	R
	Provide reports detailing support contractor relationships on a regularly scheduled basis per contract specifications.	CI	AR	R	R
	Participate in supplier and contract review meetings to manage supplier relationship (communications, risks, changes, failures, improvements, contracts and interfaces).	CI	AR	R	R
	Actively manage the supplier's portfolio of services by regularly reviewing, maintaining and optimizing compliance with the NGEN segmentation strategy.	CI	AR	R	R
	Evaluate supplier candidates according to predefined criteria (Government Services Administration {GSA} schedules, RFP responses, SLAs, end-user feedback, etc.)	CI	AR	R	R
	Continuously audit the supplier's contract compliance.	CI	AR	R	R
	Provide performance management plans which include monitoring of service level agreements, contract requirements and other key	CI	AR	R	R

	performance indicators.				

3.7.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Demand Management
- Service Portfolio Management
- Supplier Management
- Service Catalog Management
- Request Fulfillment
- Service Level Management

Inputs

Consider the inputs to the process:

- Underpinning Contracts
- Actual costs
- Supplier Contracts
- Supplier Contract Database
- SIPS, Survey Reports

Outputs

Consider the outputs from the process:

- Service Level Agreement
- Services needed
- Supplier information
- PBA
- Service Requirements
- Availability Plan
- Capacity Plan
- Resource needs
- Knowledge Ban
- Metrics

3.7.6 Roles

The following roles have been identified with the process.

Roles	Description
Supplier Process Owner	The strategic role that is accountable for the Process.
Supplier Process Manager (Supplier Manager)	The tactical role that performs cross Segment coordination.
Service Provider Lead	The operational role that coordinates activities and supervises resources in the performance of Process Activities within their Segment.
Supplier Management Team	The government team (PCO) that is responsible for contract renewals, termination and the risk plan.

3.7.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Reduce Contract and Supplier weaknesses and Problems	1	Number of Agreed UCs – percentage of contracts underpinned by UCs
		2	Number of Contract Reviews – number of conducted contract and supplier reviews
		3	Number of Identified Contract Breaches – number of contractual obligations which were not fulfilled by suppliers (identified during contract reviews)
2	Provide the Supplier Management Framework	4	The increase in the number of suppliers that meet contract agreements.
		5	The increase in the number of contract goals that agree with the SLA and SLR.
3	Clear ownership and awareness of supplier and contractual issues	6	Increase in the number of suppliers with nominated supplier managers.
		7	Increase in number of contracts with nominated contract managers.

3.7.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- All tools that provide reports on adherence to SLAs

4 Service Transition

Service Transition focuses on the implementation of the output of the Service design activities and the creation of a production service or modification of an existing service. There is an area of overlap between Service Transition and Service Operation. Key areas of the Service Transition volume are: Knowledge Management, Evaluation, Service Validation & Testing, Release and Deployment Management, Service Asset and Configuration Management and Change Management.

4.1 Knowledge Management

4.1.1 Process Overview

Knowledge Management is responsible for gathering, analyzing, storing, and sharing knowledge and information within an organization. The key purpose of this process is to ensure the right information is delivered to the right place or person at the right time in order to enable informed decisions. Effective Knowledge Management should reduce or eliminate the need to rediscover knowledge.

Key objectives of Knowledge Management are:

- Enabling the Service Provider to improve the service quality, reduce service cost and increase customer satisfaction
- Ensuring staff has a unified understanding of the value and benefits services provide to customers
- Ensuring staff has continuous access to adequate information service usage and consumption, service delivery constraints, and Problem information such as errors, faults and workarounds.

This process is central to providing knowledge to all other IT Service Management processes, especially during Service Transition in light of its dependency on the information and knowledge of users, the service desk, support staff and suppliers.

Knowledge Management can be visualized using the flow:

Data → Information (who, what, where, when) **→ Knowledge** (how) **→ Wisdom** (why)

4.1.2 High Level Process Model

The following diagram illustrates the high level process model.

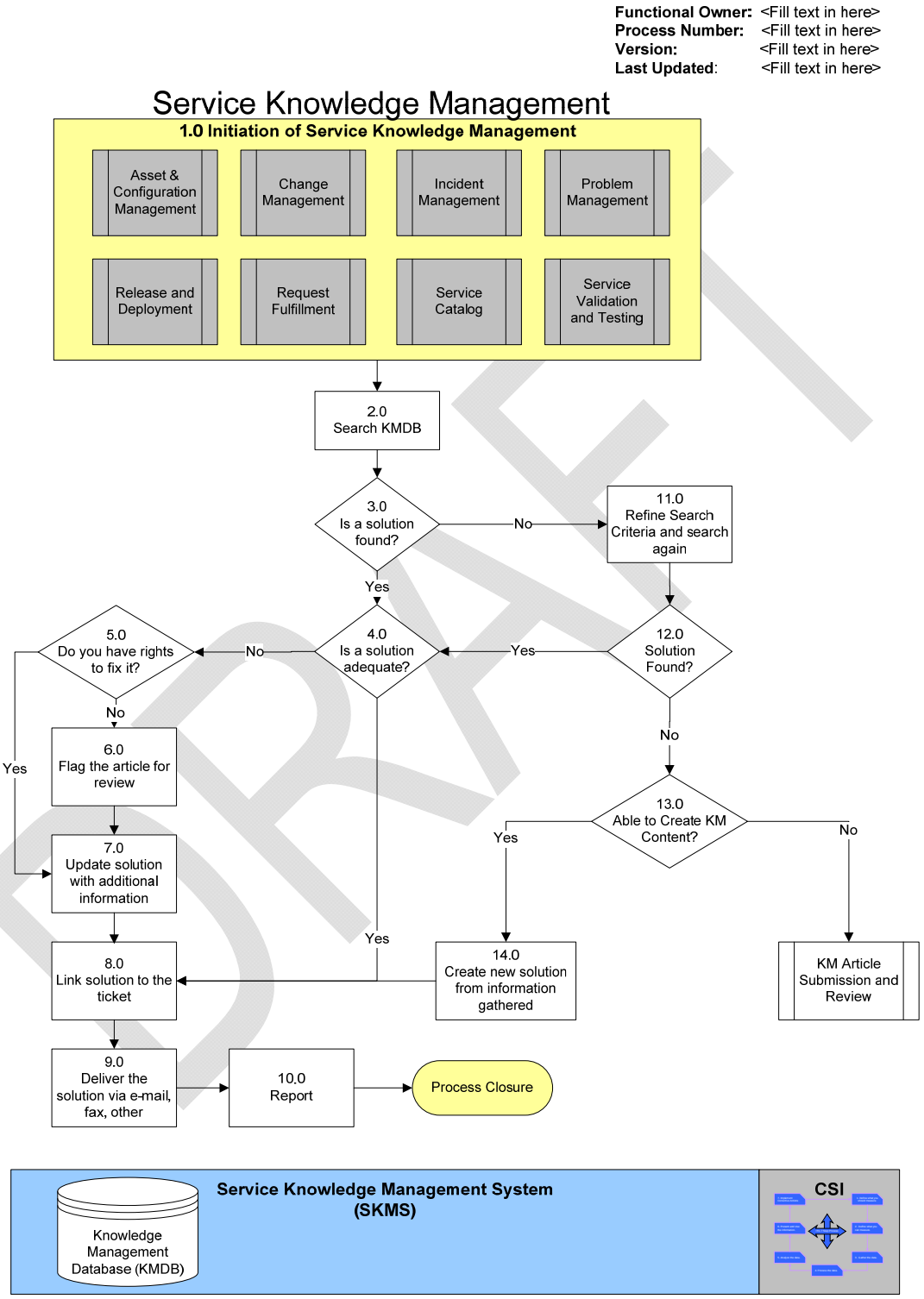


Figure 12 Service Knowledge Management Model

4.1.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of Service Knowledge Management	Develop and maintain the Service Knowledge Management System (SKMS tool). Establish and maintain content standards for the SKMS. Train and certify authors, reviewers and publishers of SKMS content. Enforce SKMS policies and procedures to protect the knowledgebase and its content.
2.0	Search Knowledge Management Database (KMDB)	Perform keyword search.
3.0	Is a solution found?	Determine whether the information exists in the KMDB.
4.0	Is a solution adequate?	Recommend content to be added to the SKMS system.
5.0	Do you have rights to fix it?	Determine whether user has rights to access information. Author new information in the SKMS system.
6.0	Flag the article for review	Review SKMS articles to ensure information is relevant, accurate and complete.
7.0	Update solution with additional information	Publish content -- Determine the level of visibility of the SKMS content (i.e. end-user visibility for self-help, tier 1, tier 2)
8.0	Link solution to the ticket	Review articles that have been flagged for review by end-user / process participants.
9.0	Deliver the solution via e-mail, fax, other	Remove outdated, sensitive or incorrect information.
10.0	Report	Generate and publish interactions related with the knowledge base (i.e. frequently used articles, articles used for end-user self help, articles appearing in search results that are not relevant).

11.0	Refine Search Criteria and search again	Enforce SKMS policies and procedures to protect the knowledgebase and its content.
12.0	Solution found?	Determine whether the information is fit for purpose.
13.0	Able to create KM content?	Determine whether user can obtain rights to create KM content.
14.0	Create new solution from information generated	Create new solution and upload to KMDB.

4.1.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	NGEN shall have a knowledge repository where the organization's collective information can be stored, searched, used and updated with a specific scope focused on IT Support Center Knowledge.
	The Service Desk shall rely heavily on this knowledgebase to resolve issues and answer questions. To achieve this goal it will be important that the full IT Service organization participate and contribute to the Knowledge Management process.
	The Service Knowledge Management System (SKMS) consisting of one or more tools shall have multiple self help interfaces for end users while allowing the service desk and support teams at all levels to search, browse, store, retrieve, update, publish, subscribe and collaborate.
	The Service Provider shall have a Knowledge Manager that will be the single point of contact for the Knowledge Management Process. This is the operational role that coordinates activities and supervises resources in the performance of Process Activities within their segment.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Knowledge Manager
	Ensure SKMS is updated as work is performed or as information is discovered.	CI	AR	R	R
	Use and/or interface with a single NGEN Enterprise SKMS tool that will be the single source of knowledge content for NGEN.	CI	AR	R	R
	Train/certify personnel sufficient to populate and maintain content of the SKMS related to their services. Certification will entail training and demonstrated capabilities to follow processes, content standards, and tool functionality, as directed by the Government.	CI	AR	R	R
	Participate in a workflow that reviews SKMS content related to their services. This review will adhere to the negotiated SLAs.	CI	AR	R	R
	Responsible for ensuring information in the SKMS is maintained, accurate and relevant.	CI	AR	R	R
	Populate the SKMS with information required by support teams to maintain availability of NGEN services. Examples of information types are: • Known Errors with systems • Troubleshooting procedures • Workarounds for Incidents / Problems • How to guides • FAQs • Manuals System Changes and updates.	CI	AR	R	R

	Have rights to modify content where appropriate or, at a minimum, the ability to flag SKMS content for review by a system administrator.	CI	AR	R	R
	Upon delivery of services, the Service Provider shall provide the information required for initial population of the SKMS.	CI	AR	R	R

4.1.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Asset and Configuration Management
- Release and Deployment Management
- Change Management
- Request Fulfillment
- Incident Management
- Service Catalog Management
- Problem Management
- Service Validation and Testing.

Inputs

Consider the inputs to the process:

- KMDB (part of SKMS)
- Actual costs
- Capacity requirements
- KEDB

Outputs

Consider the outputs from the process:

- Better cost estimates
- Updated KMDB (part of SKMS)
- Capacity Plan
- ITSCM Plan

- Contract Database
- Service Catalog
- Security Policy
- CI information
- Service Release and plans
- Test data
- SLA, OLA
- Metrics
- Incident Reports
- Errors, faults and workarounds
- CMS

4.1.6 Roles

The following roles have been identified with the process.

Roles	Description
Knowledge Management Process Owner	The strategic role accountable for the Process.
Knowledge Management Process Manager	The tactical role that performs cross segment coordination and runs the day to day, end to end Knowledge Management process.
Knowledge Manager	Operational role coordinating activities and supervising resources in the performance of process activities within their segment.
Subject Matter Experts (SME) Contributors and Reviewers	SMEs who write Knowledge Management content.

4.1.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Increase accessibility and delivery of	1	Implementation of new and changed Services

	up-to-date knowledge.		without a lot of knowledge- related errors.
		2	Increased knowledge among target groups.
		3	Higher number of answered questions.
		4	Reduced dependence on personnel for knowledge.
		5	Faster identification/location of diagnostic information about Incidents and Problems.
2	Improve collaboration and sharing knowledge that enables effective program management.	6	Shorter 'early life support'.
		7	Shorter Problem- solving times.
		8	Improved user experience.
		8	Fewer unjustified error reports due to more targeted knowledge transfer.
		10	Errors reported by personnel or through an audit.
3	Provide affordable and cost-effective knowledge delivery.	11	The use of the knowledge base, extent of re-use of documentation.
		12	Involvement of personnel in discussion and question/answer forums.

4.2 Evaluation

4.2.1 Process Overview

The purpose of the Evaluation process is to provide a consistent way of determining the performance of a service change pertaining to current and upcoming services and supporting infrastructure.

It is a generic process that considers whether the performance of something – a service or component – is acceptable, fit for purpose, financially viable. It determines the performance of a service change and evaluates service quality on a regular basis. This includes identifying areas where the targeted service levels are not reached, and holding regular talks with business to make sure the agreed service levels are still in line with the business needs.

This process delivers an important piece of input for Continual Service Improvement and the future improvement of Service development and Change Management. It includes three parts:

- Complaints Management; to assess customer complaints and to instigate corrective action if required

- Customer Satisfaction Survey; to plan, carry out and evaluate regular customer satisfaction surveys. The principal aim of this process is to learn about areas where customer expectations are not being met before customers are lost to alternative service
- Service Review; to review business services and infrastructure services on a regular basis. The aim of this process is to improve service quality where necessary, and to identify more economical ways of providing a service where possible.

4.2.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

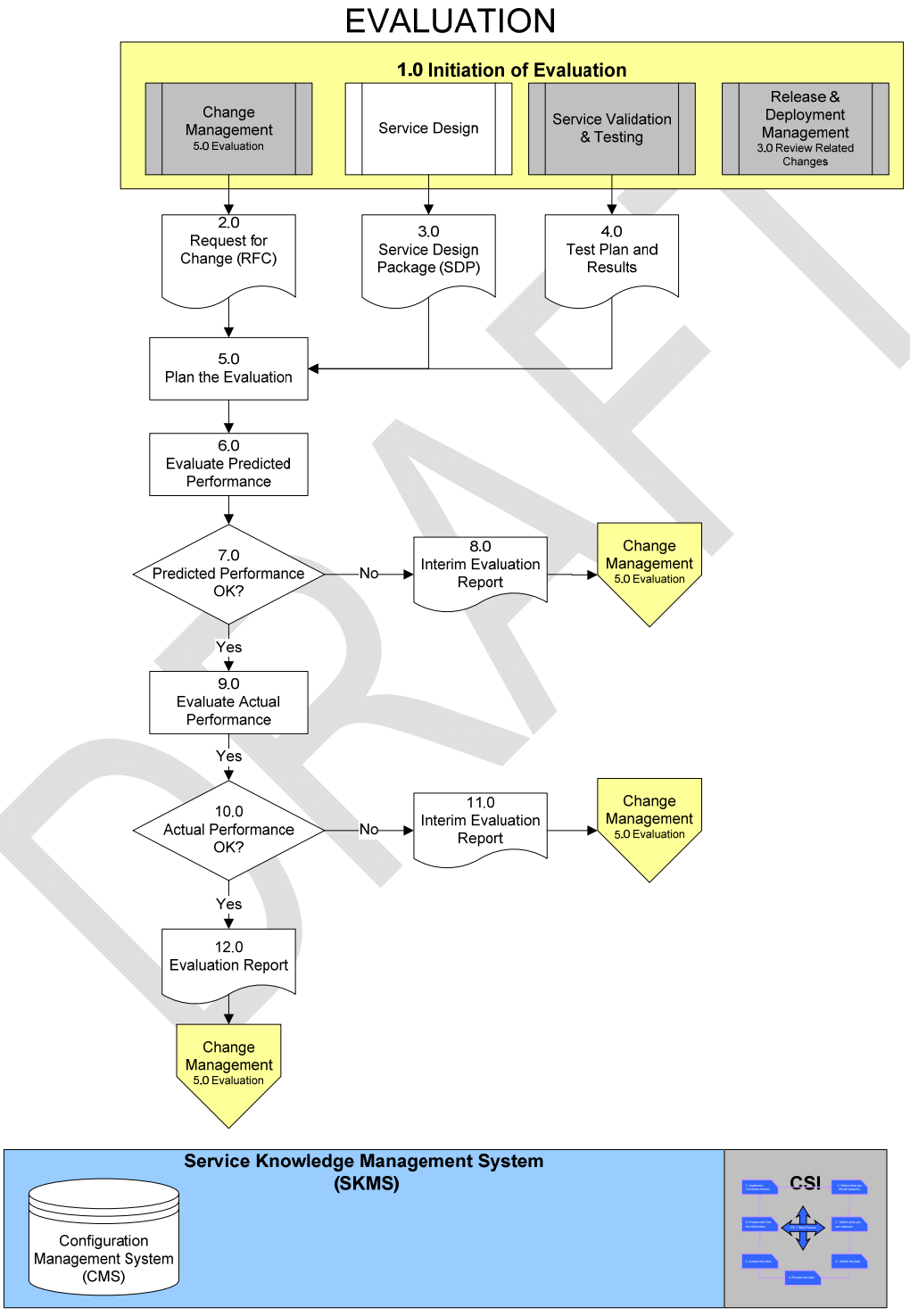


Figure 13 Evaluation Model

4.2.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiate Evaluation	Initiate the Evaluation Process from one or more of the following processes: Change Management, Service Design or Service Validation & Testing.
2.0	Request for Change (artifact)	Receive a RFC from Change Management for a change to an existing service or the introduction of a new service.
3.0	Service Design Package (artifact)	Receive a Service Design Package (SDP), which provides the acceptance criteria and predicted performance to be evaluated, from Service Design.
4.0	Test Plan and Results (artifact)	Receive the test plans and results related to the new or modified service to be evaluated from Service Validation & Testing.
5.0	Plan the Evaluation	Develop an evaluation plan appropriate for the type of evaluation. Develop a recommended list of test beds at which to perform the test.
6.0	Evaluate Predicted Performance	Evaluate the predicted performance expected from the evaluation and if the activity determines that the results are not acceptable, the evaluation is terminated and Change Management is notified of the results.
7.0	Predicted Performance OK?	Determine whether the predicted performance meets established criteria and forward findings to Change Management. Obtain decision from Change Management whether to proceed.
8.0	Interim Evaluation Report	Generate an interim evaluation report of the actual performance evaluations and acceptable results that includes recommendations. Change Management is notified of the results and is provided the final report.
9.0	Evaluate Actual Performance	Evaluate the Actual performance expected from the evaluation and if the activity determines that the results are not acceptable, the evaluation is

		terminated and Change Management is notified of the results.
10.0	Actual Performance OK?	Determine whether the predicted performance meets established criteria and forward findings to Change Management. Obtain decision from Change Management whether to proceed.
11.0	Interim Evaluation Report (artifact)	An interim evaluation report is generated of the actual performance evaluations and acceptable results that includes recommendations
12.0	Evaluation Report (artifact)	The final evaluation report is generated of the actual performance evaluations and acceptable results that include recommendations. Communicate results of final report to change management.

4.2.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	The Service Provider segment Change Manager shall be the single point of contact for each Release. This is the operational role that coordinates activities and supervises resources in the performance of Process Activities within their segment.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process	Process	Process	Service Provider	Change

	Specification	Owner	Manager	Lead	Manager
	Assist the DON with identifying the business, financial and technical criteria needed to evaluate the Service Provider's new or changed Service.	CI	AR	R	R
	Assist the DON with the planning, evaluation and reporting for all new or changed Services involving the Service Provider. This may include setting up testing environments, loading test data, and system configuration.	CI	AR	R	R
	Ensure all information related to the new or changed Service is up-to-date within the SKMS.	CI	AR	R	R
	Support the DON in evaluating deviations between predicted and actual performance for all new or changed Services.	CI	AR	R	R
	Provide Evaluation and Interim Evaluation reports at the request of the DON in a DON-defined format that contains the following sections: • Risk profile (A representation of the residual risk left after a Change has been implemented and after countermeasures have been applied) • Detailed and Summary analysis of Deviations (The difference between predicted and actual performance following the implementation of a change) • Qualification statement (proof that a change to a service does not adversely affect the quality or standards of that service or related services of other providers) • Validation statement (statement that the Service can be validated based on validation test results and a validation plan) • Recommendation (statement recommending accepting or rejecting the new or changed Service)	CI	AR	R	R

4.2.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Change Management
- Service Design
- Service Validation and Testing

Inputs

Consider the inputs to the process:

- Service Package
- Release package
- Service Design Package (SDP)
- Request for Change (RFC)
- Service Acceptance Criteria
- Test Plan and Results

Outputs

Consider the outputs from the process:

- Evaluation report

4.2.6 Roles

The following roles have been identified with the process.

Roles	Description
Evaluation Process Owner	The strategic role accountable for the process.
Evaluation Process Manager	The tactical role that performs cross segment coordination.
Change Manager	A Change Manager has the responsibility for management reports, chairing all CAB meeting, tabling RFCs, receiving, logging and allocating priority, authorizing or rejecting RFCs, establishing schedules, tracking progress and reviewing.

4.2.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Improve Customer Satisfaction	1	Number of Customer Complaints - Number of received customer complaints.
		2	Number of Accepted Customer Complaints - Number of received customer complaints which were accepted as justified.
		3	Number of Customer Satisfaction Surveys - Number of formal Customer Satisfaction Surveys carried out during the reporting period.
		4	Percentage of Returned Questionnaires - Percentage of questionnaires returned, in relation to all questionnaires being sent out.
		5	Number of Service Evaluations - Number of formal Service Evaluations carried out during the reporting period.
2	Improve accuracy in responding to Customer needs	6	Number of Process Benchmarkings, Maturity Assessments, and Audits - Number of formal Process Benchmarkings, Maturity Assessments, and Audits carried out during the reporting period.
		7	Number of Process Evaluations - Number of formal Service Evaluations carried out.
		8	Number of Identified Weaknesses - Number of weaknesses which were identified during Service Evaluation, to be addressed by improvement initiatives.
3	Increase response times to Customer	9	Variance from service performance required by customers
		10	Number of Incidents against the service
		11	Number of failed designs that have been transitioned
		12	Cycle time to perform an evaluation

4.2.8 Tools Interface Requirements

Tool interfaces requirements cannot be specified in any detail as Evaluation can be such a broad area.

4.3 Service Validation and Testing

4.3.1 Process Overview

Service Validation and Testing is a process that contributes to quality assurance and ensures that the service delivered matches its design specification and will deliver a new or changed service that is fit for purpose and fit for use.

Testing is a vital area with Service Management and has often been the unseen underlying cause of what was taken to be inefficient Service Management processes. If Services are not tested sufficiently, then their introduction into the operational environment will create and increase in Incidents, Service Desk calls for assistance, Problems and errors, costs and Service that are not used effectively by users to deliver the desired value.

The objectives of Service Validation and Testing are to:

- Assure that a release will create a service offering that delivers the expected outcomes and value.
- Confirm that the customer and stakeholder service requirements are well defined at the outset.
- Validate and assure that a service is fit for purpose and fit for use.

4.3.2 High Level Process Model

The following diagram illustrates the high level process model.

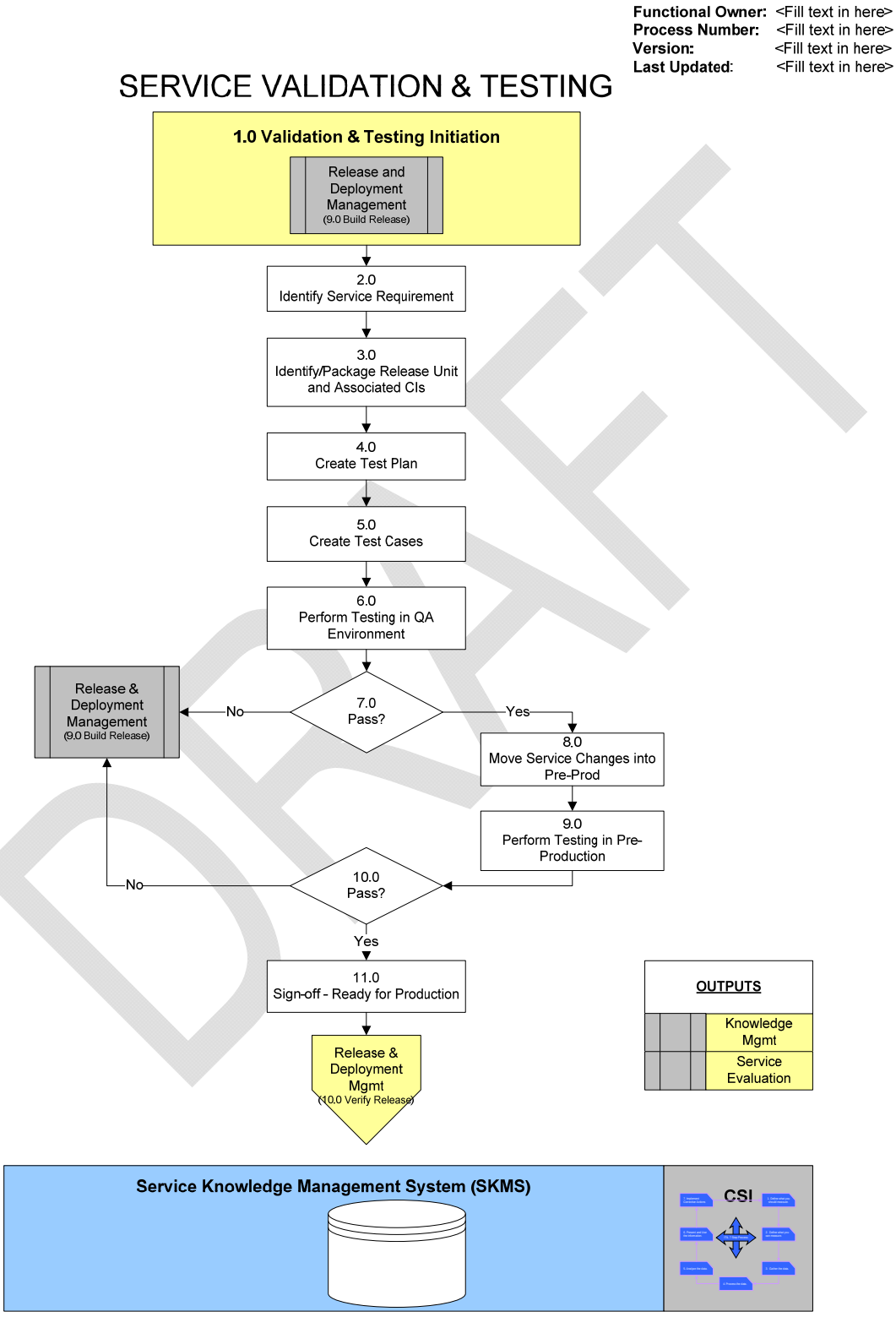


Figure 14 Service Validation and Testing Model

4.3.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Validation and Testing Initiation	Initiate the Service Validation and Testing process from Release & Deployment. Develop and maintain test environments (Minimum of 3 test environments: Development, Quality Assurance, Pre-Production).
2.0	Service Requirement	Identify Service Requirement to be tested from details provided in Release package from Release and Deployment Management.
3.0	Identify/Package Release Unit and Associated CIs	Identify the service release package contents and related Configuration Items (CIs) to fully understand service interdependencies and their configuration relationship to the Configuration Management System (CMS).
4.0	Create Test Plan	Identify any existing test cases for the service being tested and related services. Develop an integrated set of Test Cases using the existing services and any new capabilities added to the service release package.
5.0	Create Test Cases	Identify any existing test cases for the service being tested and related services. Develop an integrated set of Test Cases using the existing services and any new capabilities added to the service release package.
6.0	Perform Testing in QA Environment	Perform the tests necessary to determine proper service release operation and continuity of Services and CIs operation with acceptable performance.
7.0	Pass?	Determine whether the service meets the specified test case criteria as operated in the test environment.
8.0	Move Service Changes into Pre-Production	Move all Service components and CIs into the Pre-Production testing environment.

9.0	Perform Testing in Pre-Production	Perform the tests necessary to determine proper service release operation and continuity of Services and CIs operation with acceptable performance.
10.0	Pass?	Determine whether the release package is fit-for-purpose and fit-for-use as specified by the end user criteria. Make the decision regarding the success or failure of testing. Evaluate Exit Criteria and submit Testing Report with recommendations.
11.0	Sign-off - Ready for Production	Sign off and approve as Ready for Production Release. Clean Up Test Environments and Close. Proceed to the Release and Deployment Management process to verify release.

4.3.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following table associates the required ITSM process specifications with seams, key roles and their authority in terms of RACI (Responsible, Accountable, Consulted, Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	QA Manager
	Develop three test environments (Development, Quality Assurance (QA), Pre-Production) that mirror the production environment to support testing activities to ensure all releases are fit for use.	CI	AR	R	R
	Develop Service Requirements	CI	AR	R	R

	(technical and functional) that the testing team can use in creating test cases for all releases (Quarterly, Monthly and Emergency).				
	Provide required system documentation and work with the Testing team to train them on the system functionality and performance.	CI	AR	R	R
	Participate in Test Plan reviews to ensure adequate test coverage and an appropriate test approach.	CI	AR	R	R
	Develop test cases and reviews of test plans developed by QA teams and consult QA teams as required.	CI	AR	R	R
	Participate in the Test Summary review for each release (Quarterly, Monthly and Emergency).	CI	AR	R	R
	Participate in risk assessment meetings and risk mitigation planning.	CI	AR	R	R

4.3.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Release and Deployment Management
- Change Management
- Knowledge Management

Inputs

Consider the inputs to the process:

- Actual costs
- Managed impact on Demand
- Quality of Services
- Availability requirements
- Capacity requirements
- Testing Data
- Resource needs

- Quality Assurance
- Testing results and issues
- CMS
- Service Testing
- Test data
- Test validation data
- Review process

Outputs

Consider the outputs from the process:

- Cost estimates
- Service information
- Contract Database
- Catalog updates
- Security Policy
- RFC
- CI information
- Services releases requirements
- SKMS
- SLA, OLA
- Metrics
- Root Cause analysis

4.3.6 Roles

The following roles have been identified with the process.

Roles	Description
Service Validation & Testing Process Owner	The strategic role accountable for the Service Validation & Testing process.
Service Validation & Testing Process Manager	The tactical role responsible for cross-segment coordination.
QA Manager	A Quality Assurance Manager is accountable for assuring quality requirements will be validated through testing.

4.3.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Identify issues at an early stage of the lifecycle.	1	Number of identified errors per release during release testing.
		2	Level of impact from Incidents and errors post-deployment.
		3	Number of Incidents caused by new release.
2	Build quality into every phase of the lifecycle, for example using the V model.	4	Percentage of failed service acceptance tests.
		5	A better understanding by all stakeholders of the roles and responsibilities that relate to the new or changed service.
		6	Time for Error Fixing - Time until re-submission of fixed release components.
3	Using reusable test models to provide validation that all configurations have been built and implemented according to client requirements.	7	Percentage of Failed Release Component Acceptance Tests.
		8	Percentage of Failed User Acceptance Tests (UATs).
		9	Number of known errors documented during prior test phases.

4.3.8 Tools Interface Requirements

Tool interfaces requirements cannot be specified in any detail as Service Validation and Testing can be such a broad area.

4.4 Transition Planning and Support

4.4.1 Process Overview

Transition Planning and Support aims to plan and coordinate resources to ensure the work in service strategy and service design is realized in service operations with the minimum of impact and disruption. It is a break-out Process from Release & Deployment Management.

The objectives of this process are:

- Planning and coordinating capacity and resources to place a new or changed service into production within the triple restraints of time, cost and quality

- Ensuring all teams use established processes and tools in order to improve the planning and coordinating
- Aligning or connecting transition plans to change (project) plans of clients, suppliers and the business.

This process will enable the management of high volumes of changes and releases across NGEN.

4.4.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

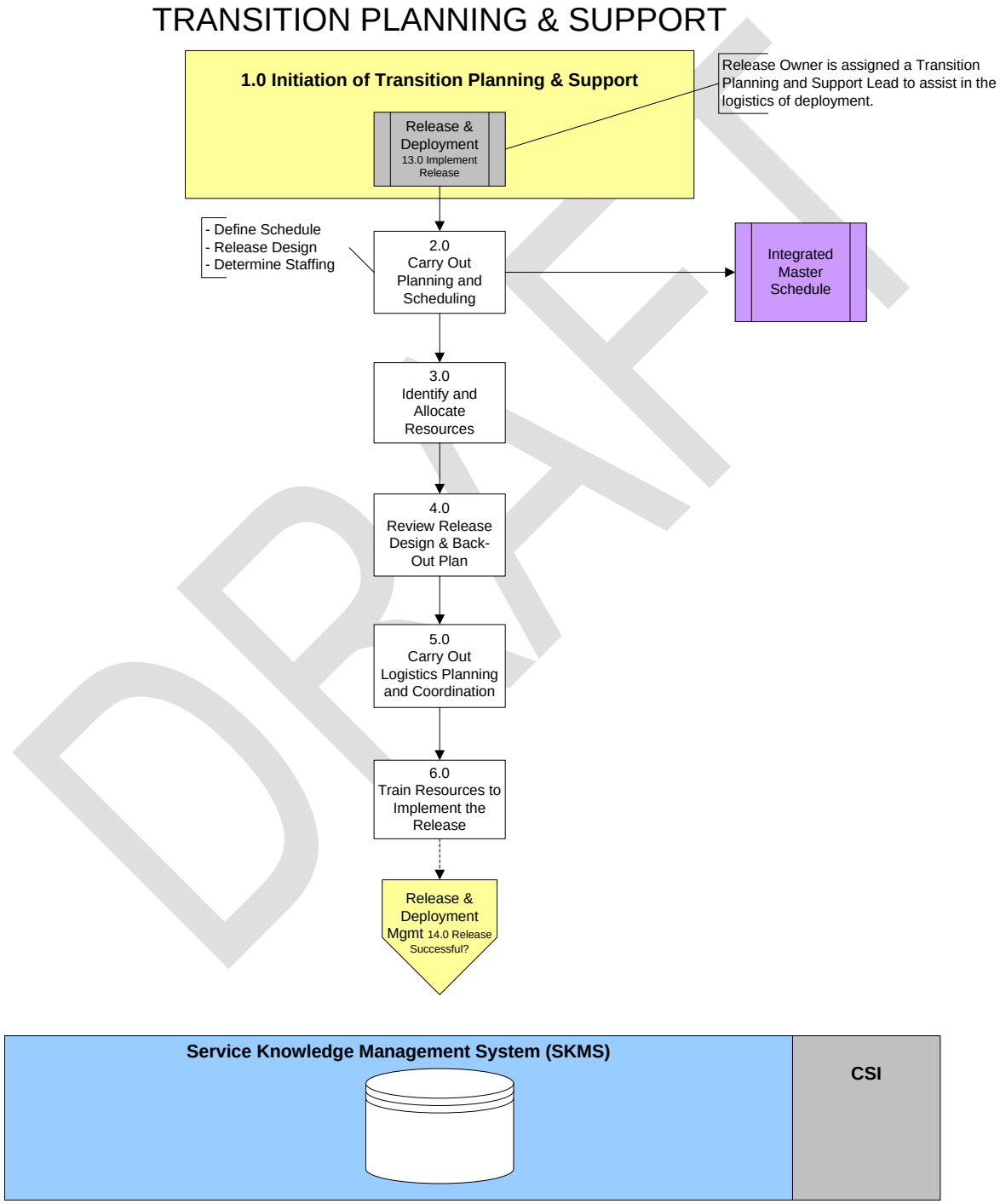


Figure 15 Transition Planning and Support Model

4.4.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of Transition Planning & Support	Incorporate design and operation requirements into transition plan. Manage and operate Transition Planning and Support activities. Maintain and integrate Service Transition plans across the customers, service, and contract portfolios. Manage Service Transition progress, changes, issues, risk, and deviations. Review Service Transition, Release, and Deployment plans. Manage and operate the transition processes, supporting systems, and tools. Communicate with customers, users, and stakeholders. Monitor and improve Service Transition performance.
2.0	Carry Out Planning and Scheduling	Establish release policies and procedures. Define release roles and responsibilities of all staff. Define responsibilities of central Release Management staff. Define tools to support the release of hardware and software into the live environment. Identify Staff to support Release Management.
3.0	Identify and Allocate Resources	Allocate specific resources to the activities and modify the plan to fit in with any new circumstances.
4.0	Review Release Design & Back-Out Plan	Document in plan how changes are going to be applied to production and how changes can be backed out if Problems occur.

5.0	Carry Out Logistics Planning and Coordination	Determine the strategy for how each release is defined and then brought into existence in a state ready for deployment. Consider the constituents of the release (from one or more Service Packages). Consider the impact of the one or more authorized changes that relate to the release contents in order to create the overall plan for the release.
6.0	Train Resources to Implement the Release	Determine transition preparation and training requirements. Plan the education and training program related to the service request. Assign and schedule training and knowledge transfer.

4.4.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	The coordination of a Release across all segments shall be led by a Release Owner in DON.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager (Release Manager)	Service Provider Lead
	Ensure resources assist in the deployment (transition into production)	CI	AR	R

	of the new or change services. These resources will act under the direction of the Release Owner.			
	Assist in developing the training materials required to train deployment staff.	CI	AR	R

4.4.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Release and Deployment Management

Inputs

Consider the inputs to the process:

- Transition Policies
- Authorized RFCs
- Service Design Package

Outputs

Consider the outputs from the process:

- Transition Strategy
- Service Transition plans

4.4.6 Roles

The following roles have been identified with the process.

Roles	Description
Transition Planning and Support Process Owner	The strategic role accountable for the Transition Planning and Support process
Transition Planning and Support Process Manager (Release Manager)	The tactical role responsible for cross-segment coordination. The role responsible for being the lead technical resource, signing-off release to production, assisting in rollout planning, organizing testing and acceptance criteria, and controlling the release package.
Service Provider Lead	The segment process representative, acting an the operational role coordinating activities and supervising resources in the performance of process activities within

	their segment.

4.4.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Rollout a timely, quality and successful release.	1	The number of implemented releases that comply with client specifications.
		2	Increased client and end-user satisfaction regarding plan and communications.
		3	Decrease in the number of deviations with respect to intended scope, quality, costs and resources.
		4	Decrease in the number of issues, risks and delays as a result of improved planning.
2	Use a project management method to carry out releases	5	Percentage of major release rollouts under the control of project management.
		6	Percentage of projects with a signed Project Charter in place.
3	Reduce the amount of poor changes to transition plans.	7	Percentage of unsuccessful changes to the transition plan.
		8	Percentage of unauthorized changes to the transition plan.
4	Improve control of release costs and timelines.	9	Adherence to Project Budget Actual vs. planned consumption of financial and personnel resources
		10	Project Delays Actual vs. planned project completion dates

4.4.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- N/A

4.5 Release and Deployment Management

4.5.1 Process Overview

The goal of Release and Deployment Management is to build, test and deploy releases into production, to handover to service operation and to establish effective use of the service in order to deliver value to the customer.

Release Management is the process responsible for planning, scheduling, and controlling the movement of releases to test and live environments. Its primary objective is to ensure that the integrity of the live environment is protected, and that the correct components are released.

Deployment is the activity responsible for movement of new or changed hardware, software, documentation and processes to the live environment. The term rollout is most often used to refer to complex or phased deployments or deployments to multiple locations.

The specific objectives of the process are:

- Aligning release and deployment plans with customer and business change projects.
- Successfully building, installing, testing and deploying a release package to the target environment, with the necessary documentation and training.
- Ensuring the new or changed service and underlying infrastructure are delivered to the agreed service level, ensuring the service utility, warrantee and level.
- Keeping to a minimum the impact on production services, operations and support staff and business in general.

This process attempts to reduce the struggle that IT has with consistency and quality of incorporating application and infrastructure into the production environment.

NGEN requirements state that the process and tools will:

- Introduce a new capability to support business and warfighting goals such as new functionality, minimized risk to existing functionality and service, or audit capability
- Protect the production environment and IT services through the use of formal procedures and checks that include risk assessment and mitigation of risks
- Reduce the impact of scheduled outages to the live environment by bundling multiple changes when possible
- Create a holistic view of multi-faceted changes that involve activities of multiple organizations.

NGEN will provide a Systems Integration Environment (SIE) that will provide the ability to engineer, certify, and accredit complete network solutions prior to implementation. The SIE will be an end-to-end systems integration, modeling, and test environment for hardware, software, applications, etc.

To ensure that only authorized releases are introduced into the live environment, NGEN shall ensure that release management processes and tools facilitate the planning and direction of the rollout of software, related hardware, documentation, and operating procedures, including

- Release creation
- Release installation and activation using the change management process
- Large hardware/software rollouts
- Bundling or batching of related changes using the change management process
- Protecting the live environment
- Verification of successful installation
- Rollback and back-out.

4.5.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

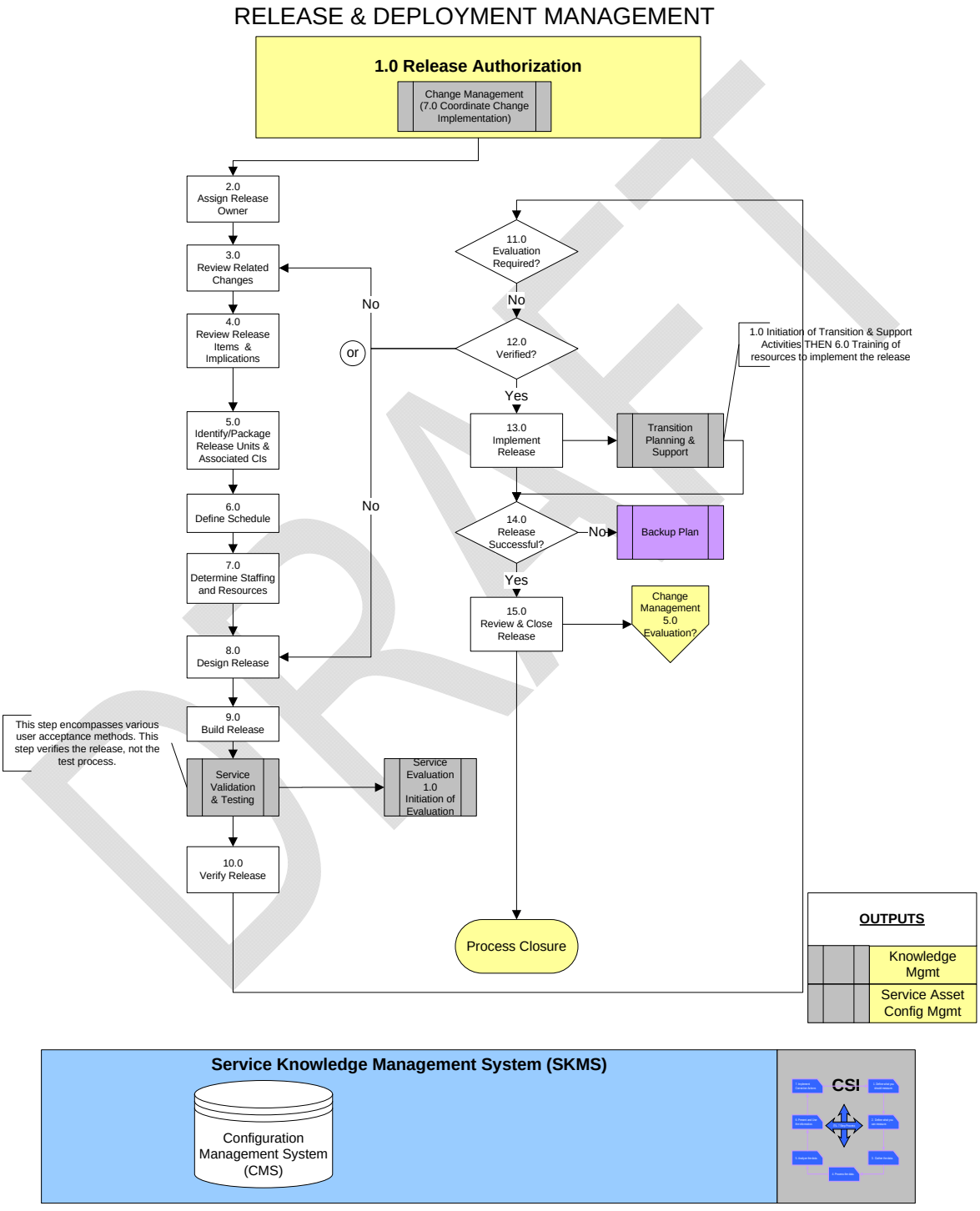


Figure 16 Release and Deployment Management Model

4.5.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Release Authorization	Authorize one or more related RFCs to be considered as a release package for authorization, scheduling and release.
2.0	Assign Release Owner	Assign one or more related RFCs to a Release Owner to formally define the release and shepherd it through the Release & Deployment Management Process.
3.0	Review Related Changes	Review the change record related to the release as well as recent change requests to determine which ones should be enacted as part of the release. A release may include a single change or multiple changes. Complex changes may need to be rolled out as part of multiple releases.
4.0	Review Release Items and Implications	Review the set of items, including product packages, which are to be released. Determine whether those items should be put into a single release, multiple releases, etc. Identify the implications of the release, including working relationships with other processes and teams.
5.0	Identify/Package Release Unit and Associated CIs	Work with Change Management and Asset & Configuration Management to determine which changes will go into the release and identify and analyze all new and changed CIs that will comprise the release
6.0	Define Schedule	Determine the schedule for the release. There should be enough time in the release schedule to handle implementation of back-out plans. Coordinate release schedule with NGEN's Integrated Master Schedule (IMS).
7.0	Determine Staffing and Resources	Determine how the implementation of the release will be staffed and determine other resources needed. Identify resource availability issues. Determine resource tradeoffs.
8.0	Design Release	Define the activities, timescales, resource requirements and responsibilities required to

		implement the release.
9.0	Build Release	Establish a build environment that replicates the production environment so that all of the new and changed CIs that comprise the release can be tested together.
10.0	Verify Release	After Service Validation and Testing, verify that the release achieves the actual desired outcome(s) within the specified technical parameters, e.g. meets fit-for-purpose requirements.
11.0	Evaluation Required?	Verify that the release achieves the actual desired outcome(s) within the specified technical parameters, e.g. meets fit-for-purpose requirements.
12.0	Verified?	Determine whether the Release package requires a formal Evaluation (Service Evaluation Process)?
13.0	Implement Release	Determine whether the release is verified successfully. Return to step "Review Related Changes" if the release is not verified successfully.
14.0	Release Successful?	Update all Configuration Items (CIs) in the CMS system prior to the release. Deploy the Release package into the production environment.
15.0	Review & Close Release	Determine if the release needs to be modified. Identify improvements that need to be made. Update the SKMS with any relevant information related to the release, known errors, or specific actions required by support teams. Examine the information relating to the usage of a release in order to identify what has worked well and what has not. This activity includes checking the actual performance and outcomes of the new or changed service against the requirements. Review and Close Deployment. Return to Change Management step "Evaluation".

4.5.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service

Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

. The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	All Service Provider will have a Release and Deployment Management team (Segment Process representative) that will be the single point of contact for each Release.
	The Release Owner shall coordinate all Releases and the Service Provider shall use or interface with the Government's ITSM toolset.
	The Service Provider shall assign a Release Owner who manages the design, testing, scheduling and roll-out of the Release under PM NGEN's direction. The Release Owner is also responsible for coordinating the cross-segment resources necessary to implement the Release.
	The Service Provider's Release and Deployment Management team works closely with the DON's Process Manager in researching and addressing process failures or to identify changes that would better meet the needs of the organization(s).

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Release Manager
	Support an Enterprise Change Management process that will approve all changes prior to a change being released into the production environment.	CI	AR	R	R
	Provide weekly updates on release related tasks assigned to them. These updates will be recorded using the DON's tool along with any additional	CI	AR	R	R

	communication required by the Release Owner.				
	Update all necessary CI details within the DON's CMS prior to changes being released into the production environment.	CI	AR	R	R
	Update the Service Knowledge Management System (SKMS) with relevant information related to release and deployment activities or Changes (i.e. known defects, known issues, new functionality, training materials, troubleshooting guides, Frequently Asked Questions) before changes are released into the production environment.	CI	AR	R	R
	Ensure that the Release Schedule is an input into the Integrated Master Schedule (IMS).	CI	AR	R	R
	Assist in developing training for end users and support teams prior to a release containing significant changes such as added functionality or feature changes.	CI	AR	R	R
	Assist in reviewing release items to identify release packages and develop the release schedule under the direction of the Release Owner.	CI	AR	R	R
	Participate in design and build of a release package as it pertains to their services. This would include coordinating with other Service Providers.	CI	AR	R	R
	Participate in a Risk Assessment of the release package to determine risks, triggers, and impacts.	CI	AR	R	R
	Support structured release schedule of Major Releases quarterly, Minor Releases monthly and Emergency Releases as required.	CI	AR	R	R
	Build the release packages related to their service(s) according to the determined release schedule.	CI	AR	R	R
	Provide assistance to NGEN PM at the time of release to verify and validate a	CI	AR	R	R

	successful deployment of the changes. The Government (DON) will be responsible for initiating and completing all releases.				
	Provide assistance to the Releases Owner in developing back-out plans in the event that a Release fails.	CI	AR	R	R
	Assist in deployment of the back-out plan in the event of a failed release and collaborates with other Service Providers across segments as required by the Release Owner.	CI	AR	R	R
	Report to the Service Desk all Incidents caused by a change/release and assists Incident Management teams to resolve Incidents caused by the change (as required by Incident Management).	CI	AR	R	R
	Provide input into the Release Owner's "Release Summary Report" that identifies any failures, lessons learned, risks, recommendations or other relevant information.	CI	AR	R	R

4.5.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Transition Planning and Support
- Change Management

Inputs

Consider the inputs to the process:

- Release schedule and notification
- Actual costs
- Impact on demand of releases
- Release planning
- Release Notification
- Release Notification and requirements

- Service releases
- Security Policy and guidance
- Release requirements
- Release plans
- Service Transition Reports
- Transition reviews
- Information on upcoming releases
- Notice of release

Outputs

Consider the outputs from the process:

- Notification of releases
- SKMS
- Cost estimates
- Effect on Patterns of Business Activity
- Portfolio updates
- Impact on service availability
- Advice on distribution strategies
- ITSCM Plan
- Contract Database
- Catalog updates
- Release Notification
- Control of Releases
- SKMS
- SLA, OLA
- Metrics
- Targets for improvements
- Performance of some minor changes
- Service Support
- Reports on Incidents per release
- Reports on Problems introduced by new release

4.5.6 Roles

The following roles have been identified with the process.

Roles	Description
Release and Deployment Management Process Owner	The strategic role accountable for Release and Deployment management.
Release and Deployment Management Process Manager	The tactical role responsible for cross-segment coordination.
Release Manager	A Release Manager has the responsibility for being the lead technical resource, signing-off release to production, assisting in rollout planning, organizing testing and acceptance criteria, and controlling the release package.

4.5.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Implement Releases Efficiently and Effectively	1	Release Efficiency Rate. NGEN will need to assess and report on how efficient releases are handled. = Calculated by Total number of releases implemented divided by the Total number of releases in the pipeline.
		2	Release Success Rate. NGEN will need to assess and report on how successful it is at implementing releases. = 1 minus the Number of failed releases divided by the Total number of releases implemented.
		3	Release Reschedule Rate. NGEN will need to assess and report on how well releases are implemented on schedule. = Number of releases rescheduled divided by the Total number of releases in the pipeline.
		5	Release Labor Utilization. NGEN will need to ensure sufficient labor capacity to support releases properly. = Total labor hours expended to implement releases divided by the Total release labor hours available.
		6	Release Management Tooling Support Level.

			The NGEN toolset will effectively support release management activities. COBIT maturity model.
		9	Release Withdraw Rate. NGEN will need to assess and report on the percent of releases that never go into production. = Number of releases withdrawn divided by the Total number of releases in the pipeline.
		10	Release Labor Waste Rate. NGEN will need to minimize labor waste when planning and implementing releases. = The sum of the Number of failed releases, Number of releases resulting in Incidents and the Number of releases withdrawn all divided by the Total number of releases in the pipeline.
2	Implement High Quality Releases	2	Release Success Rate. NGEN will need to assess and report on how successful it is at implementing releases. = 1 minus the Number of failed releases divided by the Total number of releases implemented.
		4	Release Defect Rate. NGEN will need to assess and report on the percentage of releases that cause Incidents. = Number of releases resulting in Incidents divided by the Total number of releases implemented.
		6	Release Management Tooling Support Level. The NGEN toolset will effectively support release management activities. COBIT maturity model.
		8	Number of Known Release Errors. NGEN will ensure all releases are of the highest quality before releasing them into production. = Number of Errors for Pareto analysis.
3	Provide a Repeatable Process for Releases	6	Release Management Tooling Support Level. The NGEN toolset will effectively support release management activities. COBIT maturity model.
		7	Release Management Process Maturity Level. NGEN will efficiently and effectively conduct release management practices. COBIT maturity model.

4.5.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Configuration Management System
- Change Management and Service Desk System
- Definitive Media Library

4.6 Service Asset and Configuration Management

4.6.1 Process Overview

The purpose of Service Asset and Configuration Management is to define and control the components of services and infrastructure and to maintain accurate configuration information on their historical, planned and current state.

This process is responsible for identifying, controlling, recording, tracking, reporting, auditing and verifying the value and ownership of service assets throughout their lifecycles, and for maintaining information about CIs (Configuration Items) required to deliver an IT Service (including their relationships).

Configuration Management involves identifying configuration of all items in a system such as software, hardware components, data, documentation, at a given starting point in time. It then proceeds with the systematic control of configuration changes and maintains the integrity and traceability of the configuration baseline throughout the lifecycle.

Assets will be managed in accordance with DoD practices; where this is lacking; asset management will be in accordance with applicable best practices in sections of ISO 20000 and be guided by applicable sections of the Information Technology Infrastructure Library (ITIL).

Accordingly, NGEN shall provide worldwide support for deployed equipment and software to meet the specified availability in equipment support. Methods used to meet the specified availability may include, but are not limited to, pre-positioning of spares, deploying replacement units, using forward “points of service,” providing online troubleshooting, or using deployed Naval/Marine Corps maintainers.

NGEN shall establish asset management processes that will at a minimum provide:

- IT asset evaluation and selection
- IT asset procurement processes that consider software pricing, contracts, and licensing, hardware pricing, contracts, and leasing and also service level agreements
- IT asset maintenance and support, including hardware and software
- IT asset disposal
- Intellectual property management
- Software maintenance and support
- IT asset management software.

4.6.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

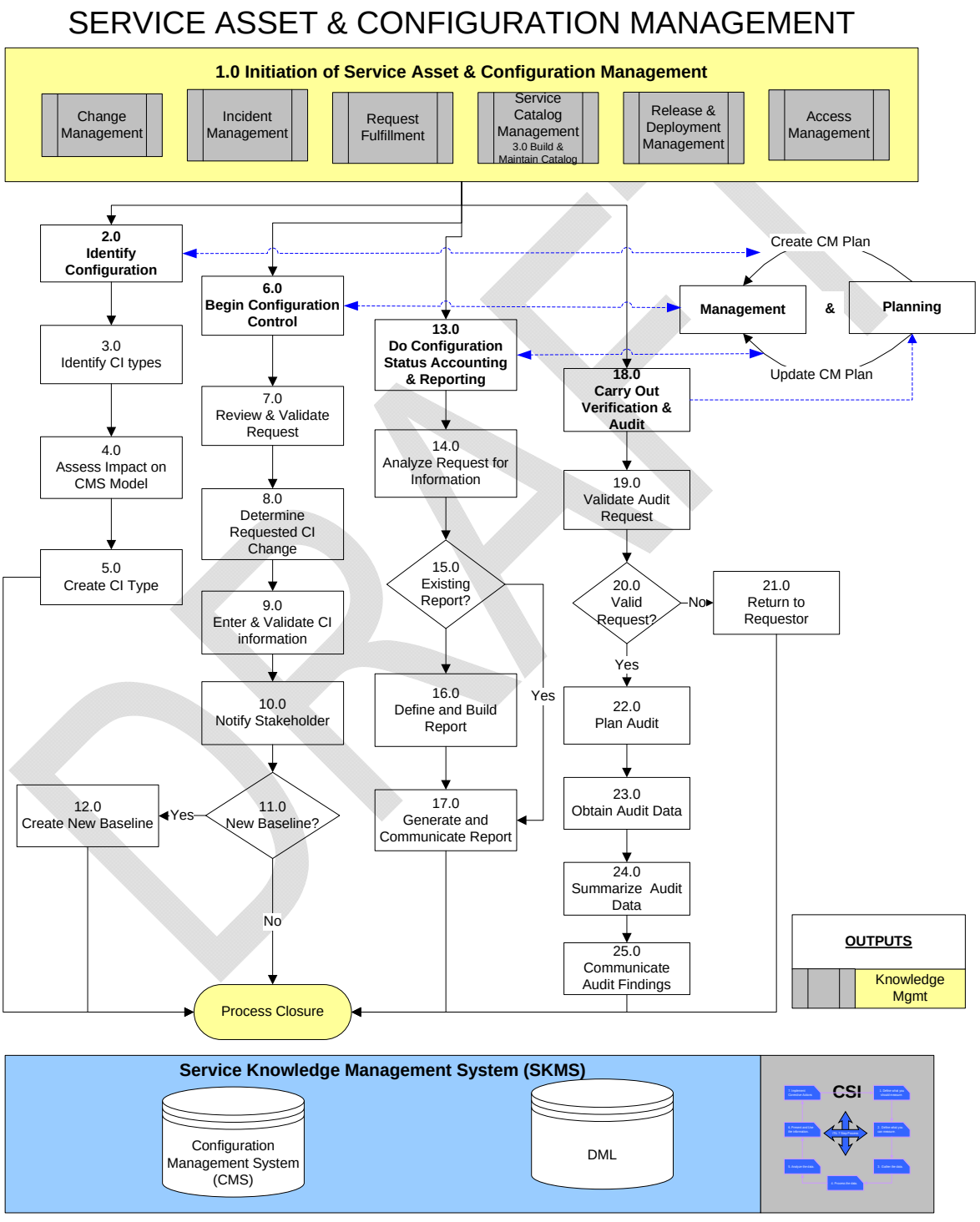


Figure 17 Service Asset and Configuration Management Model

4.6.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of Service Asset & Configuration Management	Asset Management coordinates the asset lifecycle of all assets. Information about assets is kept within the Asset Register (which contains much information that is also found within the CMDB). Configuration Management focuses on the various elements (CIs) in the IT infrastructure and their relationships, managing the integrity of all CIs and maintaining accurate information about them. Assets and CIs are overlapping concepts (the Asset Register and the CMDB can be based on some similar underlying physical data models, but are logically different).
2.0	Identify Configuration	Define how the classes and types of assets and CIs are to be selected, grouped, classified, and defined by appropriate characteristics (e.g., warranties for a service to ensure that they are manageable and traceable throughout their lifecycles). Define the approach to identification, uniquely naming and labeling all assets or service components of interest across the service lifecycle, and the relationships between them.
3.0	Identify CI Types	Define the types of CIs under the control of Configuration Management. • During the initial population of a CMDB within the CMS (this discovery can be done manually or automatically). • When a new type of CI is identified for inclusion within the CMS (as a result of design at either the architectural level or within a particular solution, a new CI type can be generated that should be reflected within the CMS schema). Once a new type of CI is identified, a number of steps might need to occur, including:

		• Creating specific naming conventions for this CI type. • Creating specific labeling conventions. • Defining attributes for the CI type. • Defining documentation for the CI type. • Defining relationships to other CI types. Store this information in the Configuration Identification Practices (each of the decisions can result in an update to or modification of the CMS schema, resulting in a proposal to update the CMS).
4.0	Assess Impact on CMS Model	Baselines are added to the CMS as they are developed. Changes to baselines and the release of work products built from the CMS are systematically controlled and monitored via the configuration control, Change Management, and configuration auditing functions of the SACM.
5.0	Create CI Type	There should be a consistent and commonly understood definition of what constitutes a CI and the reasons for management by configuration function.
6.0	Begin Configuration Control	No CI should be added, modified, replaced, or removed without appropriate controlling documentation or procedure being followed.
7.0	Review & Validate Request	Uncover, define, formalize, negotiate, validate, and agree service requirements as they relate to the prevailing service request.
8.0	Determine Requested CI Change	Establish the CI change that has been requested.
9.0	Enter & Validate CI information	Store information about IT infrastructure CIs in the CMS when creating new CI records or when updating or deleting existing CI records. Record all transactions in specific parts of the CMS.
10.0	Notify Stakeholder	Ensure that SACM information is accurate to trigger approval and notification transactions for decision-making via workflow tools (e.g., changes

		or acceptance of deliverables) Send a service notification to: • Inform relevant parties that the release package is available for installation and use. • Communication the change to relevant stakeholders.
11.0	New Baseline?	Determine whether a new baseline is needed. The way CIs move from one state or another should be defined (e.g., an application release may be registered, accepted, installed, or withdrawn).
12.0	Create New Baseline	Create configuration of a service, product, or infrastructure that has been formally reviewed and agreed upon, that thereafter serves as the basis for further activities, and that can be changed only through formal change procedures. Captures the structure, contents, and details of a configuration and represents a set of CIs that are related one to another.
13.0	Do Configuration Status Accounting and Reporting	Ensure that all configuration data and documentation is recorded as each asset or CI progresses through its lifecycle (this provides the status of the configuration of a service and its environment as the configuration evolves through the service lifecycle).
14.0	Analyze Request for Information	Analyze Request for Information.
15.0	Existing Report?	Determine whether a canned report already exists.
16.0	Define and Build Report	Receive and Process requests for asset reports: • These can include ad hoc or standard reports. • As needed, design, generate, and disseminate asset reports as per request. Make CI and CMS information available to any authorized requestor: • This information can range from detailed attributes and relationships to summarized information. • It can cover an individual CI or a collection of

		CIs. • It can be essentially unformatted raw data or predetermined reports. • It can be provided in line with a planned schedule or in response to an individual request.
17.0	Generate and Communicate Report	Generate report to communicate changes to CIs.
18.0	Carry Out Verification & Audit	Ensure that there is conformity between documented baselines (e.g., agreements and interface control documents) and the actual business environment to which they refer.
19.0	Validate Audit Request	Consider configuration audits at the following times: • Shortly after changes to the CMS. • Before and after changes to IT services or infrastructure. • Before a release or installation in order to ensure that the environment is as expected. • Following recovery from disasters and after a "return to normal" (this audit should be included in contingency plans). • At planned intervals. • At random intervals. • In response to the detection of any unauthorized CIs.
20.0	Valid Request?	Determine whether a request is valid based on pre-determined criteria.
21.0	Return to Requestor	Notify requestor that the request is not justified by existing audit guidelines.
22.0	Plan Audit	Planning for an audit involves four major activities: • Verifying the reference model to be used for the audit is relevant and industry acceptable. • Establish a baseline reference point by assessing the current situation. • Prepare a detailed report for the difference

		between the reference model and the current situation in the form of a gaps analysis supported by a risk analysis and plan of action. • Schedule a program of initiatives to remedy items with a significant level of risk of compliance related importance.
23.0	Obtain Audit Data	Determine the reference model to be used for an audit against which the organization's policies, procedures, and Processes will be compared.
24.0	Summarize Audit Data	Document clearly the exceptions noted. Include a risk analysis of the consequences of any gaps. Make it very clear what remediation is required in order to meet the minimum requirements of the reference model. Prioritize the recommended courses of action.
25.0	Communicate Audit Findings	Communicate audit findings to stakeholders.

4.6.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	The Service Provider shall provide a segment Service Asset & Configuration Management representative that will be the single point of contact for this Process. This is the operational role that coordinates activities and supervises resources in the performance of process activities within their segment.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager (Asset & Configuration Manager)	Service Provider Lead
	Use/interface with a single DON owned CMS that will be the single source of records for all Configuration Items (CIs).	CI	AR	R
	Populate (prior to delivery of a new service) the initial attributes and relationships in the CMS for all CIs pertaining to that service (e.g. unique identifier, CI type, name/description, version, location, supply date, license details, owner/custodian, status, supplier/source, related document masters, related software masters, historical data, relationship type, applicable SLAs).	CI	AR	R
	Provide (upon delivery of services) the information required for initial population of the CMS e.g. serial number, serviced tag number, model number and description.	CI	AR	R
	Update the attributes and relationships in the CMS for all CIs pertaining to that service upon any change to an existing service.	CI	AR	R
	Employ an auto discovery tool that will interface with a single NGEN Enterprise CMS that will be the single source of record for all Configuration Items (CIs).	CI	AR	R
	Provide a baseline of all impacted CIs prior to Release of a new or modified Service to the live environment.	CI	AR	R
	Provide a baseline of all CIs delivered, upon request.	CI	AR	R

	Adhere to the DON's CI data model and naming conventions. Examples include: service classification types, relationships between CIs (e.g. assembly and component), metadata definitions, transmission protocols.	CI	AR	R
	Update the CMS to track moves, repairs, installations (warranty/non-warranty), changes and system retirement ire upon delivery of services.	CI	AR	R
	Deliver assets with a Radio Frequency ID (RFID) tag per the DoD policy July 2004 (the exact RFID needs to be clarified)	CI	AR	R
	Support ad-hoc and regular DON audit activities (e.g. Functional Configuration Audit, Configuration Control, Configuration Status Accounting, and Physical Configuration Audit)	CI	AR	R
	Provide the following reports on a weekly basis in a format specified by the DON: (i) Detailed and Summary baseline reports containing detailed CI information by CI and by products and services, (ii) Detailed and Summary revision and status reports containing details of current revision status and change history, (iii) Detailed and Summary delivery reports containing details of the status of all delivered products and services containing part and traceability numbers, (iv) Detailed and Summary reports containing all instances of unauthorized usage of hardware and software, (v) Detailed and Summary reports of all variations between the CMS and audit reports	CI	AR	R

4.6.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Incident Management
- Change Management
- Access Management
- Request Fulfillment
- Service Catalog Management
- Release and Deployment Management

Inputs

Consider the inputs to the process:

- Actual costs
- Changes to update assets or any CI
- Changes to Service Catalog or CMS
- Major releases
- Service requirements
- Essential assets and spares that the business depends on

Outputs

Consider the outputs from the process:

- Cost estimates
- Patterns of business activity
- Updates to CMS
- Detection of point of failure
- Capacity Plan
- Contract Database
- Service information
- Updated KMDB (Knowledge Management Database, part of SKMS)
- SLAs, OLAs
- Targets for improvement
- Metrics
- Reporting
- Service Requests
- Updated Infrastructure

- Updated application databases
- Updated KEDB (Known Error Database, part of SKMS)

4.6.6 Roles

The following roles have been identified with the process.

Roles	Description
Service Asset and Configuration Management Process Owner	The strategic role accountable and responsible for the Service Asset and Configuration Management Process.
Service Asset and Configuration Management Process Manager	The tactical role responsible for cross-segment coordination and running the day-to-day, end-to-end implementation of the Service Asset and Configuration Management Process.
Service Asset and Configuration Manager	The operational role responsible for maintaining the process, assets and other CIs, proposing and establishing naming conventions, planning and organizing the population, and overseeing the management of the CMS.

4.6.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Control Information About the IT Infrastructure and Services	1	CMS Accuracy Ratio. NGEN will ensure the accuracy of information in the CMS. = 1 minus Number of CIs errors discovered divided by the Total number of CIs in the CMS.
		4	SACM Tooling Support Level. The NGEN toolset will effectively support SACM activities. COBIT maturity model.
		5	SACM Process Maturity Level. NGEN will efficiently and effectively conduct SACM practices. COBIT maturity model.
2	Support Delivery of Quality IT Services	2	Number of Incidents Related to Inaccurate CI Information. NGEN will automatically report in a timely manner how many Incidents were

			related to inaccurate CI information. Remedy is used for both ONENet and NMCI. FSETs and CASREPs are also used.
		3	Number of Change Failures Related to Inaccurate CI Information. NGEN will minimize changes that fail due to inaccurate CI information. (RFC implementation and ECCB tracking data are used in NMCI.)
		4	SACM Tooling Support Level. The NGEN toolset will effectively support SACM activities. COBIT maturity model.
		6	CMS Completeness Ratio. NGEN will ensure completeness of information in the CMDB and metrics developed to assess how complete configuration information. = 1 minus Number of services operating with incomplete CI information divided by the Number of services in the Service Catalog.
		7	CI Ownership Rate. NGEN will be required to report how much of the infrastructure has no assigned ownership. = 1 minus Number of CIs without assigned ownership divided by the Total number of CIs in the CMS.

4.6.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- The CMS is a set of tools and databases for managing IT Service Provider's configuration data and should also include data on Incidents, Problems, known errors, changes, and releases, and possibly staff, suppliers, locations, business units, customers, and users.
- The CMS will interface with or include an asset repository, an Incident Management system, a Change Management system, a DML (Definitive Media Library), an asset procurement (ordering) system and an auto-discovery tool.
- Auto-discovery dynamically updates a CMS and helps minimize its administration. It can be: agent-based, active, and passive. NGEN has requirements for auto-discovery to populate the CMS, to effect provisioning, to monitor the network and manage system performance, and to manage security.
- IT Asset Discovery and Management (ITAM) will be employed to inventory Navy enterprise IT networks on a recurring basis to maintain accuracy, capture mobile or temporarily off-line assets, and identify trends in configuration changes.
- All data collected will be owned by the government. Examples: (i) IP enabled, networked devices; (ii) Device operating systems and types (servers, desktops, printers, routers, IP-

enabled devices); (iii) System configuration data (CPU, memory, serial number, etc.); (iv) Installed software and services (vendor, version, patch level); (v) Software application and database users and usage rate (Application, Users, etc.); and (vi) Server utilization rate.

- Service Catalog.

4.7 Change Management

4.7.1 Process Overview

Change Management is the Process responsible for controlling the lifecycle of all changes and works to enable beneficial changes to be made with minimal disruption to IT Services.

The objective of Change Management is to ensure changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Changes in the IT infrastructure may arise reactively in response to Problems or externally imposed requirements, e.g. legislative changes, or proactively from seeking imposed efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Change Management can ensure standardized methods, processes and procedures are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes.

Changes must be managed to reduce risk (especially important in DOD), minimize severity of business impact and strive to be successful on the first attempt. Change in an organization can be disruptive, risky and expensive and therefore should be kept to an optimally low level.

A service change is the addition, medication or removal of authorized, planned or supported service or service component and its associated documentation.

NGEN requirements state that overall Change Management Process and associated tools, for the IT environment, will:

- Minimize the risk of disruption to IT services caused by changes to the IT services
- Introduce change in a predictable, repeatable, improved, and accountable manner
- Reduce Incidents caused by changes
- Maintain open channels of communications to promote a smooth transition when change
- occurs
- Increase visibility and communication of changes to both business and support staff
- Provide accurate assessment of the cost of proposed changes before they are incurred
- Provide an improved ability to absorb a large volume of changes
- Provide an enhanced perception of the quality of IT.

4.7.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

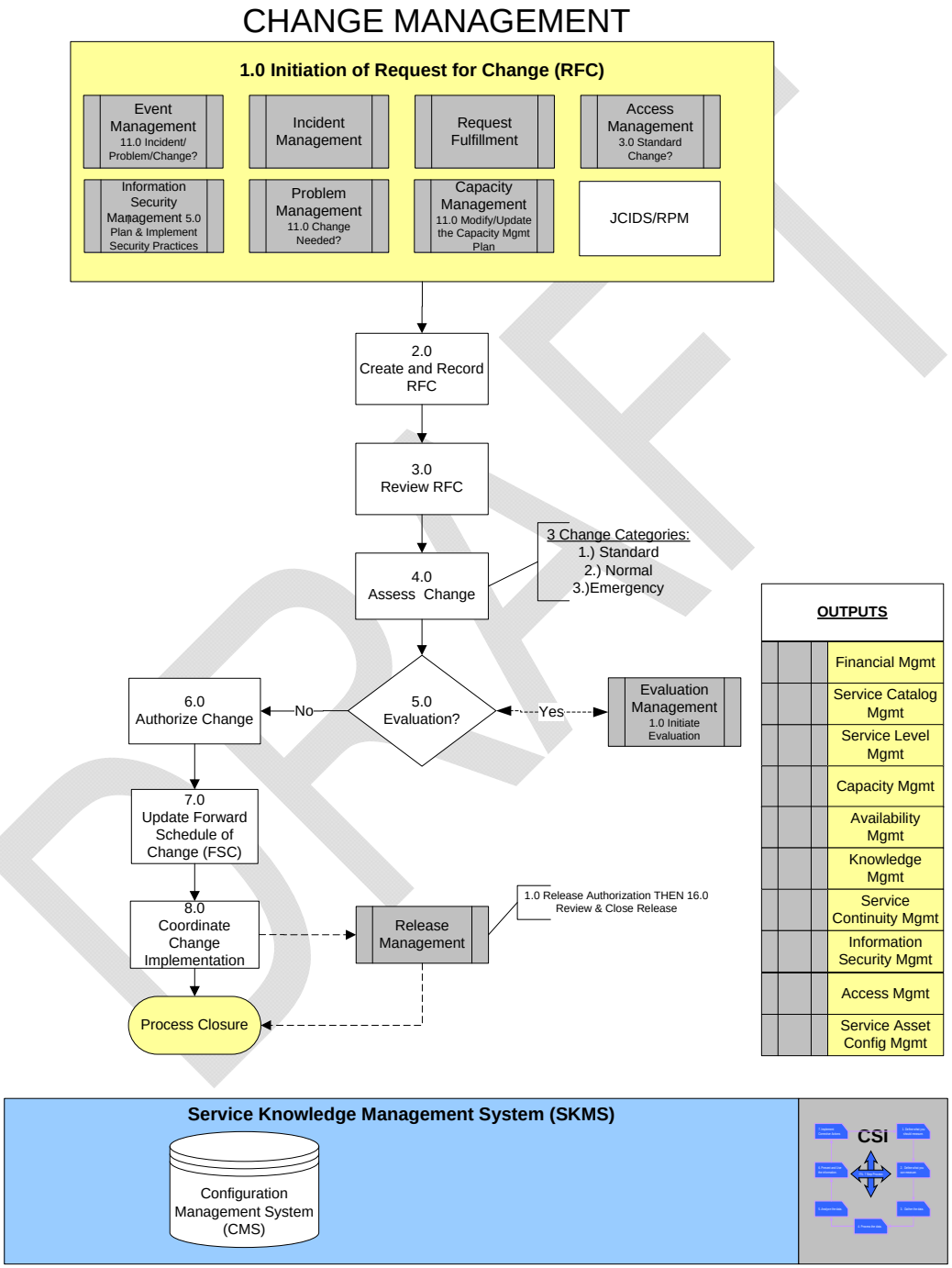


Figure 18 Change Management Model

4.7.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of Request for Change (RFC)	A change request, such as a Local Change, Regional Change or Global Change is triggered via one or more of the following processes: Incident Management, Problem Management, Request Fulfillment, Access Management, Capacity Management or Service Portfolio Management (to include the RPM process)
2.0	Create and Record RFC	Classify and prioritize RFC. Prepare estimates for time and resources required to perform the change along with projected impact to the organization
3.0	Review RFC	Review RFC for content and completeness.
4.0	Assess Change	Perform technical review and impact assessment of RFC across all services and segments (Risks, Resources, Responsibility and Relationship to other Changes.
5.0	Evaluation?	Develop back-out and/or remediation plans in the event of a change failure.
6.0	Authorize Change	Approval or Rejection by the appropriate Change authority, determined by the category of Change.
7.0	Update Forward Schedule of Changes	Coordinate Change Implementation across all segments and services by working with Release and Deployment Management, Service Validation and Testing as well as Transition Planning and Support.
8.0	Coordinate Change Implementation	Ensure change is implemented as specified and scheduled in the RFC. Ensure all affected CIs are updated in the Configuration Management System (CMS).

4.7.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	If a Request for Change requires coordination across segments, the Enterprise Change Coordination Board (ECCB) shall evaluate the impact on all segment providers as part of its Change evaluation Process. The ECCB Charter will outline specific decision and enforcement criteria, as well as a mechanism for appeal, to govern all RFCs that involve more than one Service Provider.
	There shall be representation as required to NGEN's Enterprise and/or local level CABs. The CABs shall assist in the assessment and prioritization of Changes and shall support authorization (local/enterprise) of Changes.
	There shall be segment Change representative to be the single point of contact for each Change. This is the operational role that coordinates activities and supervises resources in the performance of Process Activities within their segment. There is only ONE Lead for each Process within each segment.

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead	Change Manager
	Use or interface with the DON's NGEN Enterprise Change Management Tool to ensure there is a single source record for all Changes. All Changes will be entered, updated and tracked in this single Tool.	CI	AR	R	R
	Appoint a segment Change Manager.	CI	AR	R	R
	Provide resources on a weekly basis at a time and place designated by the DON to participate in the technical review and impact assessment of RFCs.	CI	AR	R	R

	Provide Change Management support for the following types of Changes for the purposes of prioritization and resource management: (i) Normal – Enterprise level Change requiring full CAB approval and coordination (e.g. server configuration change), (ii) Emergency – operationally imperative changes needed to protect or restore services (e.g. Global Network Operating Center {GNOC} and MCNOSC approval required).	CI	AR	R	R
	Assist end user representatives, other segment Change Managers as required, Engineering SMEs, the NGEN Change Manager, etc. to appropriately document, submit, and champion changes through provision of the following: (i) RFC, (ii) Change implementation plan, (iii) Change back-out plan, (iv) Anticipated customer impact analysis	CI	AR	R	R

4.7.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Incident Management
- Problem Management
- Request Fulfillment
- Access Management
- Capacity Management
- Service Portfolio Management
- Service Asset and Configuration Management

Inputs

Consider the inputs to the process:

- Event Report
- Incident Report
- Service Requests
- Security Report

- Problem Report
- Request to meet demand
- Actual costs
- Policy and strategy for change and releases
- Plan for change and release
- Security Report
- Proposal for change
- Request for change
- Request to meet demand
- Forward Schedule of Changes
- Service requirements
- Relating of Problems to CI /updated CI
- Control of Releases
- Test Results and Reports
- Request to update knowledgebase (part of SKMS)
- Incident Report
- Event Report
- Problem Report

Outputs

Consider the outputs from the process:

- Cost estimates
- Updated Service information
- Request for Change (RFC)
- Approved RFC
- Rejected RFC
- Change to services
- New, modified or deleted assets or CIs
- Change Record and Reports
- Release schedule and notification
- Updated KMDB (part of SKMS)
- Improved Metrics

- Strategies for improvement
- Performance of service requests
- Knowledge and expertise

4.7.6 Roles

The following roles have been identified with the process.

Roles	Description
Change Management Process Owner	The strategic role accountable for the Change Management process.
Change Management Process Manager	The tactical role responsible for cross-segment coordination.
Change Manager	A representative acting as the single point of contact for each Change.
Change Advisory Board (CAB)	Group who assesses, prioritizes and approves (or denies) changes and gives expert advice to Change Management on the implementation of changes. This board is composed of members representing both the Service Provider organization and the DON.
Emergency CAB	This CAB focuses on emergency changes only.

4.7.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Make Changes Efficiently and Effectively	1	Change Efficiency Rate. NGEN will achieve high efficiency in how changes are made. = Total number of changes implemented divided by the Total number of changes in the pipeline.
		2	Change Success Rate. NGEN will report how effectively changes are handled. = 1 minus Number of failed changes divided by the Total number of changes implemented.
		5	Average Process Time Per Change (Days). NGEN will minimize the number of days it

			takes to process changes.
		9	Change Management Tooling Support Level. The NGEN toolset will effectively support the change management process activities. COBIT maturity model.
2	Protect Services When Making Changes	3	Emergency Change Rate. NGEN will report what percentage of changes were emergencies. = Number of emergency changes divided by the Total number of changes in the pipeline.
		6	Unauthorized Change Rate. NGEN will ensure that all changes go through the change management process unless it is covered by request fulfillment, Incident management, capacity management, continuity management and event management processes. = Number of unauthorized changes detected divided by the Total number of changes in the pipeline.
		7	Change Incident Rate. NGEN will report what percentage of changes caused Incidents. = Number of changes resulting in Incidents divided by the Total number of changes implemented.
3	Utilize a Repeatable Process for Handling Changes	3	Emergency Change Rate. NGEN will report what percentage of changes were emergencies. = Number of emergency changes divided by the Total number of changes in the pipeline.
		6	Unauthorized Change Rate. NGEN will ensure that all changes go through the change management process unless it is covered by request fulfillment, Incident management, capacity management, continuity management and event management processes. = Number of unauthorized changes detected divided by the Total number of changes in the pipeline.
		9	Change Management Tooling Support Level. The NGEN toolset will effectively support the change management process activities. COBIT maturity model.
		10	Change Management Process Maturity. NGEN will efficiently and effectively conduct change management practices. COBIT maturity model.
4	Make Changes Quickly and Accurately In Line with Customer	4	Change Reschedule Rate. NGEN will need to assess how well changes are implemented on schedule. = Number of changes rescheduled divided by the Total number of changes in the

	Needs		pipeline.
		5	Average Process Time Per Change (Days). NGEN will minimize the number of days it takes to process changes.
		7	Change Incident Rate. NGEN will report what percentage of changes caused Incidents. = Number of changes resulting in Incidents divided by the Total number of changes implemented.
		8	Change Labor Workforce Utilization Rate. NGEN will ensure sufficient labor workforce capacity to support changes. = Total labor hours spent coordinating changes divided by the Total labor hours available to coordinate changes.
		9	Change Management Tooling Support Level. The NGEN toolset will effectively support the change management process activities. COBIT maturity model.

4.7.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Change Management software
- Service Desk Incident Management Tracking system
- CMDB

5 Service Operations

Service Operations focuses on the activities required to operate the services and maintain their functionality as defined in the Service Level Agreements with the customers. Key areas in this volume are: Request Fulfillment, Event Management, Availability Management, Incident Management, and Problem Management.

5.1 Request Fulfillment

5.1.1 Process Overview

Request fulfillment is the process that incorporates all aspects of fulfilling a customer's request for service. It should include self-service for identifying available services, capture the service request, approval, tracking, provisioning, delivery and delivery confirmation.

Request fulfillment is the process for handling and implementing service requests. Now a separate process from Incident management, it creates value in its ability to offer quick and effective access to standardized, predefined services needed by an organization. Its aim is to reduce the amount of "red tape" encountered in requesting and receiving access to new or existing services, ultimately reducing the cost and time necessary to deliver requested services. Since service requests occur on a regular basis, process flows, workflows, necessary approvals, individuals or teams involved, time limits and escalation paths are predefined.

The objectives of Request Fulfillment include:

- To provide a channel for users to request and receive standard service for which a pre-defined approval and qualification process exists
- To provide information to users and customers about the availability of services and the procedures for obtaining them
- To source and deliver the components of requested standard services (e.g. licenses and software media)
- To assist with general information, complaints or comments

While specific process tasks, approvals, workflow activities, and metrics vary according to the type of service being requested, the overall request fulfillment process consists of four basic activities or steps: catalog selection, financial approval, fulfillment and confirmation.

Smaller organizations may be able to rely upon their service desk support to handle both Incidents and service requests. But for larger enterprises, including service requests in the Incident management process is counterproductive. The two are incompatible because the overall goal of the enterprise is to reduce the number of Incidents yet the number of service requests will always continue steadily or grow along with customer needs.

Having a separate process and tool capability is necessary to properly manage service requests. Incident management can focus on handling Incidents or trouble tickets. Change management can focus on handling requests for change (RFC). Having clearly defined processes for these three areas goes a long way towards alleviating the confusion and chaos that result in the absence of a proper request fulfillment process. Integrating request fulfillment with other operational

processes such as access and service asset & configuration management prevents gaps and cascading complexities from occurring downstream.

Large organizations have organizational units that require different service offerings and service agreements even though they receive services from the same set of IT technical services and IT providers. The Service Catalog combined with the request fulfillment process should support these differences with capabilities such as tailored views of the catalog and tailored approval and workflow requirements. Some organizations may want to limit the service offerings available to its members or impose different approval requirements for service requests. This is a powerful new concept introduced by ITIL V3 and another reason that the Service Catalog must drive request fulfillment.

The following are considerations for the Process development where the Service Provider:

- Provides a channel to request and receive standard services for which a predefined approval and qualification scheme exists.
- Provides information to customers and users about the availability and the procedures for obtaining services.
- Sources and delivers the components of requested standard services.
- Assists with general information, complaints and comments related to their services.
- Monitors the request fulfillment system and will respond to escalated requests within defined SLAs.
- Maintains the Service Catalog related to their service and keeps ordering information current.
- Updates the Configuration Management System (CMS) for configuration items (CIs) related to their service when a request impacts a CI or an asset.

5.1.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

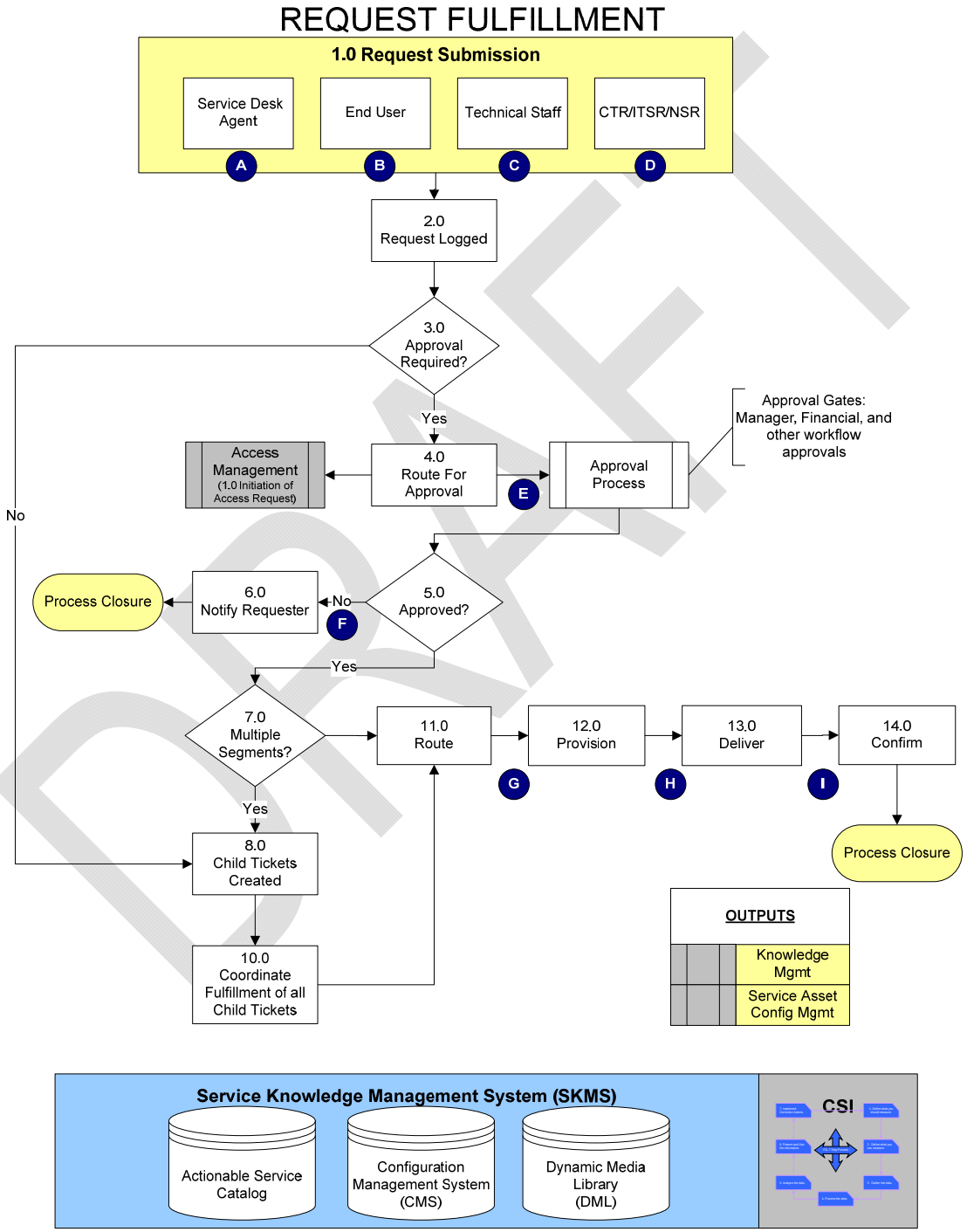


Figure 19 Request Fulfillment Model

5.1.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Request Submission	The request fulfillment process works in conjunction with the Service Catalog so that requestors can submit requests via a graphical user interface (GUI) directly into a service management system. The interface of the service management system should offer a role-based menu-like selection capability complete with service configuration and shopping cart-like tools that guide users in making selections and entering necessary details. This approach offers ideal opportunities for self-help and other efficiencies. It also allows users to see and query service related descriptions and other specifications and sets delivery expectations by displaying and using service level agreement (SLA) targets. Service Requests occur frequently and require handling in a consistent manner in order to meet agreed service levels. To assist this, many organizations create pre-defined Service Request models (which typically include some form of pre-approval by Change Management). This is similar in concept to the idea of Incident models, but applied to Service Requests.
2.0	Request Logged	The service request is logged into the Request Fulfillment tool and a Request record is created.
3.0	Approval Required?	The service request is evaluated according to a pre-defined approval and qualification process.
4.0	Route for Approval	Depending on the approval workflow required, the service request is routed to the appropriate decision-maker for approval.
	Approval Process	Most service requests have financial implications. The cost of the service being requested along with the cost of delivering and supporting it throughout its lifecycle must first be determined along with the type of chargeback model to be used to recoup

		those costs. Some services only require predefined fixed prices while more costly or complex ones require planning and estimation. Simple requests can receive quick authorizations as part of ongoing operating budgets while others may require escalation up management/financial chains for approval.
5.0	Approved?	The appropriate decision-maker(s) decide(s) to approve or reject the service request as submitted.
6.0	Notify Requestor	If the service request is rejected, the requestor is notified and possibly provided with instructions for resubmitting request or alternatives.
7.0	Multiple Segments?	Does fulfillment of the service request require cross-segment coordination?
8.0	Create Child Tickets	One or more tickets are created for the fulfillment of the service request.
10.0	Coordinate Fulfillment of all Tickets	Child tickets are coordinated to manage dependencies and optimize the critical path.
11.0	Route	The service request is routed to the appropriate support group or vendor for fulfillment.
12.0	Provision	Support groups/vendors perform all activities required to fulfill the service request.
13.0	Deliver	Delivering or implementing the requested service to the requestor is the actual fulfillment. Fulfillment activities depend on the nature of service being requested.
14.0	Confirm Delivery/Acceptance	The final step before a request can be considered complete is confirmation by the requester that the service was in fact received satisfactorily. Confirmation is a necessary step before the invoicing, billing and payment processes can be triggered.

5.1.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service

Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
A	Submission of request from Service Desk Agent to Request Fulfillment.
B	Submission of request from End-User to Request Fulfillment.
C	Submission of request from Technical Staff to Request Fulfillment.
D	Submission of request from CTR/ITSR/NSR to Request Fulfillment.
E	Forwarding the request for official approval to the designated authority.
F	Notification to requester of request denial.
G	Routing request to Vendor.
H	Provisioning segment communicates with delivery segment that a request is ready for handoff (this seam does not exist when one segment is providing both provisioning and delivery.)
I	Government confirms acceptance of service delivery.

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead
A	Use or interface with the Government (DON) Service Catalog (and single user front end) to ensure there is a single source record for all requests. The Government (DON) will capture time of submission, receipt delivery and acceptance.	CI	AR	R

B	Use or interface with the Government (DON) Service Catalog (and single user front end) to ensure there is a single source record for all requests. The Government (DON) will capture time of submission, receipt delivery and acceptance.	CI	AR	R
C	Use or interface with the Government (DON) Service Catalog (and single user front end) to ensure there is a single source record for all requests. The Government (DON) will capture time of submission, receipt delivery and acceptance.	CI	AR	R
D	Use or interface with the Government (DON) Service Catalog (and single user front end) to ensure there is a single source record for all requests. The Government (DON) will capture time of submission, receipt delivery and acceptance.	CI	AR	R
E	Forward workflow determined by origin (e.g. claimant) of request and type of request (e.g. pre-defined hardware, etc.). Approval workflows are defined by individual claimants.	CI	AR	R
F	Document the status of an order upon any status change at near real time.	CI	AR	R
G	Acknowledge receipt and commit to fulfill request within agreed upon Service Level Agreements.	CI	AR	R
H	Acknowledge receipt and commit to fulfill request within agreed upon Service Level Agreements. Support a tiered pricing structure based on the Government (DON) defined levels of urgency by service. Support delivery time set by Service dependent lead time(s). Enable Touch Labor to fulfill requests whenever possible e.g. granting access to password reset systems and ordering systems. Support purchase order/change, delivery order/change, cancellation and	CI	AR	R

	return(s) based on Government (DON) defined policies and procedures. Coordinate with the Government (DON) Transition Planning and Support process.			
I	Support purchase order/change, delivery order/change, cancellation and return(s) based on Government defined policies and procedures.	CI	AR	R

5.1.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

Service Asset & Configuration Management. There is a strong link between the request fulfillment and asset and configuration management processes. Any changes and statuses introduced by a service request must be recorded and updated in the configuration management system (CMS) as they occur.

Access Management. Requests for user accounts involve security policies and requirements maintained by access management.

Service Catalog Management. Since the Service Catalog is the starting point for all service requests it must be kept accurate and up to date to reflect available service offerings and support request fulfillment approvals and workflows.

Service Level Management. Certain SLAs are defined that determine allotted times for approvals, delivery lead-times, and status updates. Adherences to these and any breaches are managed by the service level management process.

Knowledge Management. Following the request fulfillment process requires a number of instructions, procedures and guidelines, many of which require keeping customers/requestors informed so they know how to request a service and what to expect as it is approved, delivered and confirmed. Keeping customers/requestors informed helps reduce the number of aborted requests, maintain customer satisfaction and improve SLA performance.

Inputs

Consider the inputs to the process:

- Service request
- Service Desk
- SLA
- CMS
- Service Catalog

- Security Policies

Outputs

Consider the outputs from the process:

- Fulfilled request
- Updated CMS
- RFC

5.1.6 Roles

The following roles have been identified with the process.

Roles	Description
ACNO NGEN Service Delivery IPT Process Owner and Process Manager.	This is the strategic role that is accountable for the process overall. Ensures that the process is implemented in a standardized and repeatable manner. PM Service Delivery IPT is responsible for the approval workflow and the request fulfillment tool.
NNWC and MCNOSC Process Manager(s).	This is the tactical role that performs cross-segment coordination and runs the day-to-day, end-to-end process implementation activities.
NGEN Service Provider	• Provides a Request Fulfillment Manager who will be a point of contact for escalations, Service Level Management (SLM) compliance, customer satisfaction, and will participate in the DON defined and managed Continual Process Improvement. Participation will include proactively making recommendations for process improvement. • Uses or interfaces with the DON's Request Fulfillment Tool (and single user front end) to ensure there is a single source record for all requests. • Maintains capability to respond to all escalated requests through the Government's Request Fulfillment Tool. • Captures time of submission, receipt delivery and acceptance. • Documents the status of an order upon any status change at near real time. • Enables the Service Desk to fulfill requests whenever possible e.g. granting access to password reset systems

	and ordering systems. • Enables the Touch Labor to fulfill requests whenever possible e.g. granting access to password reset systems and ordering systems. • Supports a tiered pricing structure based on the DON defined levels of urgency by service. The Service Provider will support delivery time set by Service dependent lead time(s). • Coordinates with the DON's Transition Planning and Support process. • Supports purchase order/change, delivery order/change, cancellation and return(s) based on DON defined policies and procedures.

5.1.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Every service request follows an established process.	1	Ratio of open/total number of requests
2	Timeliness of service request completion.	2	Ratio of fulfilled/aborted requests
3	Customer satisfaction rates over completion of service request.	3	Average time of approval, fulfillment, and confirmation

5.1.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- The Request Fulfillment Tool shall provide a built-in model to support order request, approval, scheduling and delivery of service through workflow automation and process control capabilities.
- The Tool shall support a request prioritization schema.
- Customers shall have the ability to create and submit service requests using web-based self-service tools

- Individuals responsible for request fulfillment shall have access to the Customer Relationship Management (CRM) tool used for Request Fulfillment
- Individuals responsible for request fulfillment shall have access to the Service Catalog
- Individuals responsible for request fulfillment shall have access to the Asset and Configuration management system (CMS).
- Individuals responsible for request fulfillment shall have access to the Change Management system for any requests or changes that are beyond the scope of request fulfillment.

The single most important best practice for request fulfillment is enabling users or requestors to go to a web-enabled self-service portal to search, compare, learn, decide, make requests and track them through their fulfillment. This is another reason that request fulfillment no longer needs to rely upon a service desk. Users are no longer confused over whether to call the service desk, which can also dramatically reduce calls.

This menu driven approach is achieved by publishing and maintaining the Service Catalog as a readily accessible menu of choices known as an actionable Service Catalog. Having only one actionable Service Catalog eliminates the pitfall of multiple channels for finding services and submitting requests, which is inefficient, confuses users and leads to customer dissatisfaction.

Another key toolset feature of request fulfillment is use of a “shopping cart” capability that can give users an intuitive e-commerce experience while affording the opportunity to integrate with backend financial systems. Creating a positive online experience for users making requests requires category management, search, comparison, selection guidance and configuration, status tracking, content management, user account management, and self-service configuration.

Below is an illustration of an integrated architecture that depicts IT service management toolset functionality. At the top is the customer facing web portal, which represents the actionable Service Catalog and request fulfillment.

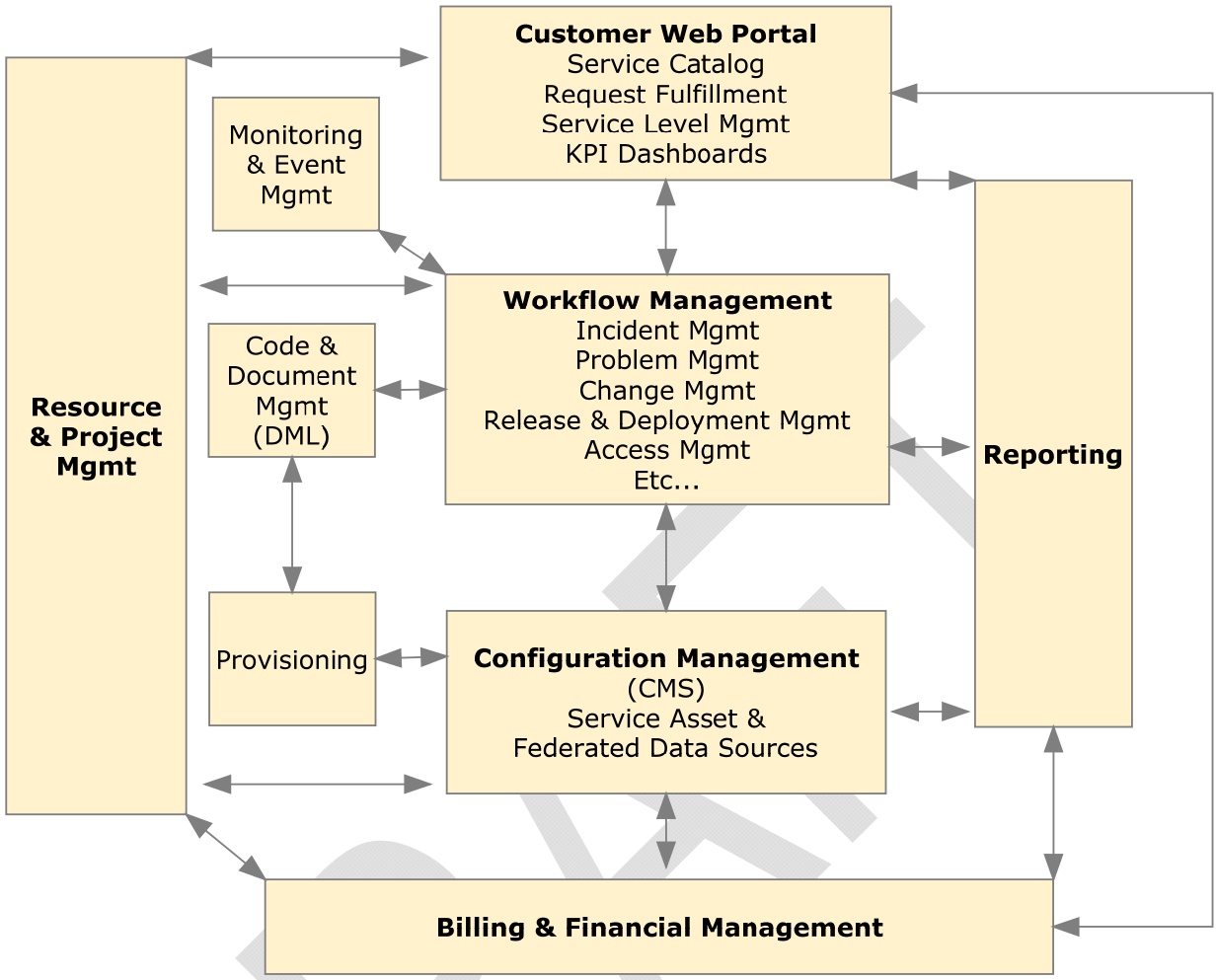


Figure 20 IT Service Management Toolset Functionality

5.2 Event Management

5.2.1 Process Overview

Event Management is the process that monitors all events that occur through the IT infrastructure to allow for normal operation and also to detect and escalate exception conditions. An event can be defined as any detectable or discernible occurrence that has significance for the management of the IT Infrastructure of the deliver of IT service. This process provides notifications created by an IT service, CI, or monitoring tool that can be programmed to communication operation information as well as warnings and exceptions, and be used as a basis for automating many operations management activities.

5.2.2 High Level Process Model

The following diagram illustrates the high level process model.

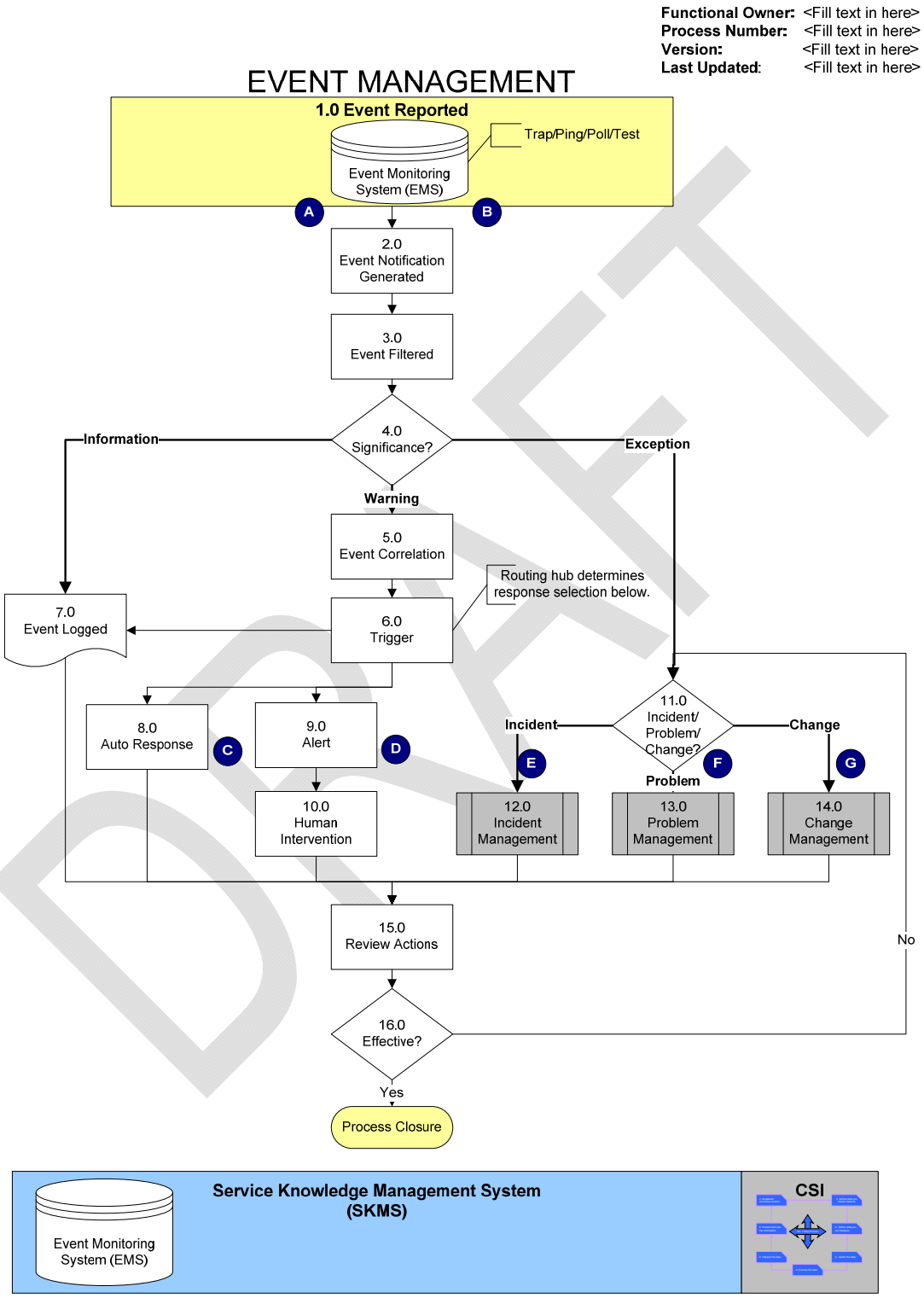


Figure 21 Event Management Model

5.2.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Event Reported	An event is defined as any detectable or discernible occurrence that has significance for the management of the IT infrastructure or delivery of IT service. Industry standard Enterprise monitoring systems such as: network monitoring tools, security management systems (e.g. intrusion detection), environmental monitoring systems, software license usage monitoring, and normal performance monitoring (e.g. server), etc.
2.0	Event Notification Generated	Monitoring systems provide notification than an Event has occurred.
3.0	Event Filtered	Determine if the Event is communicated or ignored.
4.0	Significance?	The Event is classified as Informational, Warning, or an Exception. Informational - For logging purposes only (no action required) Warning - Whenever a threshold is being approached or breached Exception - Event that is impacting the business and needs to be evaluated as a potential Incident, Problem or RFC
5.0	Event Correlation	Predefined business rules are applied to a significant Event to determine what actions are required.
6.0	Trigger	Based on Event Correlation results, specific notification/response activities are initiated.
7.0	Event Logged	The Event resulting from an entry into a device or application is recorded into the Event log.
8.0	Auto Response	A defined and automated response (e.g. rebooting and/or restarting a device, initiating a batch job, etc.)

9.0	Alert	Identifies that the Event requires human intervention and provides information required to determine appropriate action.
10.0	Human Intervention	The Event requires a person or team to perform a specific action within specified time parameters.
11.0	Incident/Problem/Change?	The Event is evaluated as a potential Incident, Problem, or Change.
12.0	Incident Management	The Event is handled by the Incident Management process.
13.0	Problem Management	The Event is handled by the Problem Management process.
14.0	Change Management	The Event is handled by the Change Management process.
15.0	Review Actions	Checks that any significant Events or exceptions have been handled appropriately. Tracks trends/counts of specific Event types. If the Event is handled by another ITIL process does not duplicate any reviews that occur within those processes.
16.0	Effective?	Was the Event handled correctly, including the handoffs to other ITIL processes and did the expected outcome occur correctly?
	Event Closure	If the Event is handed off to another ITIL process, the Event should be formally closed with a link to the appropriate record from that process.

5.2.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead
	Ensure there is a single source record for all Events. All Events will be entered, updated and tracked within the Government's Enterprise Management System.	CI	AR	R
	Have a system monitoring tool or capabilities for monitoring, detection and aggregation of global, regional, & local system, application & network events related to the system or service	CI	AR	R
	Define significant Event definitions, appropriate thresholds, and instructions for responding to significant Events for the Services provided.	CI	AR	R
	Respond to Events related to the service provided.	CI	AR	R
	Obtain weekly reports that contains the following information (the Government will have system access to generate these reports): • Total number of Events by category. • Number of Events by significance. • Number and % of Events that required human intervention and whether this was performed. • Number and % of Events that resulted in Incidents or changes. • Number and % of Events caused by existing Problems or known errors.	CI	AR	R

	• Number and % of repeated or duplicated events. • Number and % of Events indicating performance issues. • Number and % of Events indicating potential availability issues. • Number and % of each type of event per platform or application. • Number and ratio of Events compared with the number of Incidents. • Detailed and summary reports of all Events related to the service provider's service(s) that occurred during the reporting period. • Detailed and summary reports of knowledgebase articles entered as a result of Events that occurred during the reporting period.			

5.2.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Configuration Management
- Asset Management
- Knowledge Management
- Incident Management
- Problem Management
- Evaluation
- Service Level Management

Inputs

Consider the inputs to the process:

- Status change of a device
- Exceptions to any CI
- Exceptions to an automated process
- Completion of a task or job

- Status change of a device
- Management Information Basis (MIBs)

Outputs

Consider the outputs from the process:

- Management Information Basis (MIBs)
- Incident Report
- Closed Event

5.2.6 Roles

The following roles have been identified with the process.

Roles	Description
Process Owner	Accountable for ensuring that the Event Management process is fit for purpose and will achieve standardization across the NGEN enterprise. The Process Owner's responsibilities include sponsorship, process design and continual process improvement, including process metrics and reports.
Process Manager	A tactical role that is responsible to oversee the daily process activities. This person performs coordination of all Event Management activities (including cross segment involvement). S/he ensures that the current and future Event Management requirements for the enterprise are identified all critical systems are adequately and effectively monitored for events with potential impact to the delivery of services.

5.2.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Define correct level of filtering of events and alerts.	1	Number of Events and Alerts.
		2	Number of Events and Alerts that resulted in Incidents and Problems.
		3	Number of Events and Alerts caused by

			Known Errors.
2	Define thresholds together with Service Design and Service Operations.	4	Number of Events and Alerts indicating issues in other service management processes: Availability, Continuity, Performance, etc.
3	Use appropriate tools for Event and Alert Monitoring supporting automated monitoring of systems and services.	5	Number of Events and Alerts that require human intervention.
		6	Number of Events and Alerts duplicated or repeated.
		7	Number of Events and Alerts that could be solved without human intervention.

5.2.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Sufficient system monitoring tool(s) or capabilities for monitoring, detection and aggregation of global, regional, & local system, application & network events related to the system or service.
- The system monitoring tool shall integrate with the Incident Management ticketing system where Incident tickets can be automatically created and assigned to the appropriate group.

5.3 Access Management

5.3.1 Process Overview

Access Management consists of the processes and procedures responsible for allowing users to make use of IT services, systems, applications, data, or other IT assets. Access Management helps to protect the Confidentiality, Integrity and Availability of assets by ensuring that only authorized users are able to access or modify the assets. Access Management is sometimes referred to as Rights Management or Identity Management.

Key Objectives of Access Management are:

Verify identity

Provide access to authorized users

Deny access to non-authorized users

Execution of policies and actions defined in Security and Availability Management.

Grant, restrict or remove access to controlled IT services, systems, or other IT assets.

Access Management is the tactical execution of company policies relating to Information Security Management and Availability Management. Access Management is critical to IT governance and compliance and is typically managed within the IT operations function and/or Security group.

5.3.2 High Level Process Model

The following diagram illustrates the high level process model.

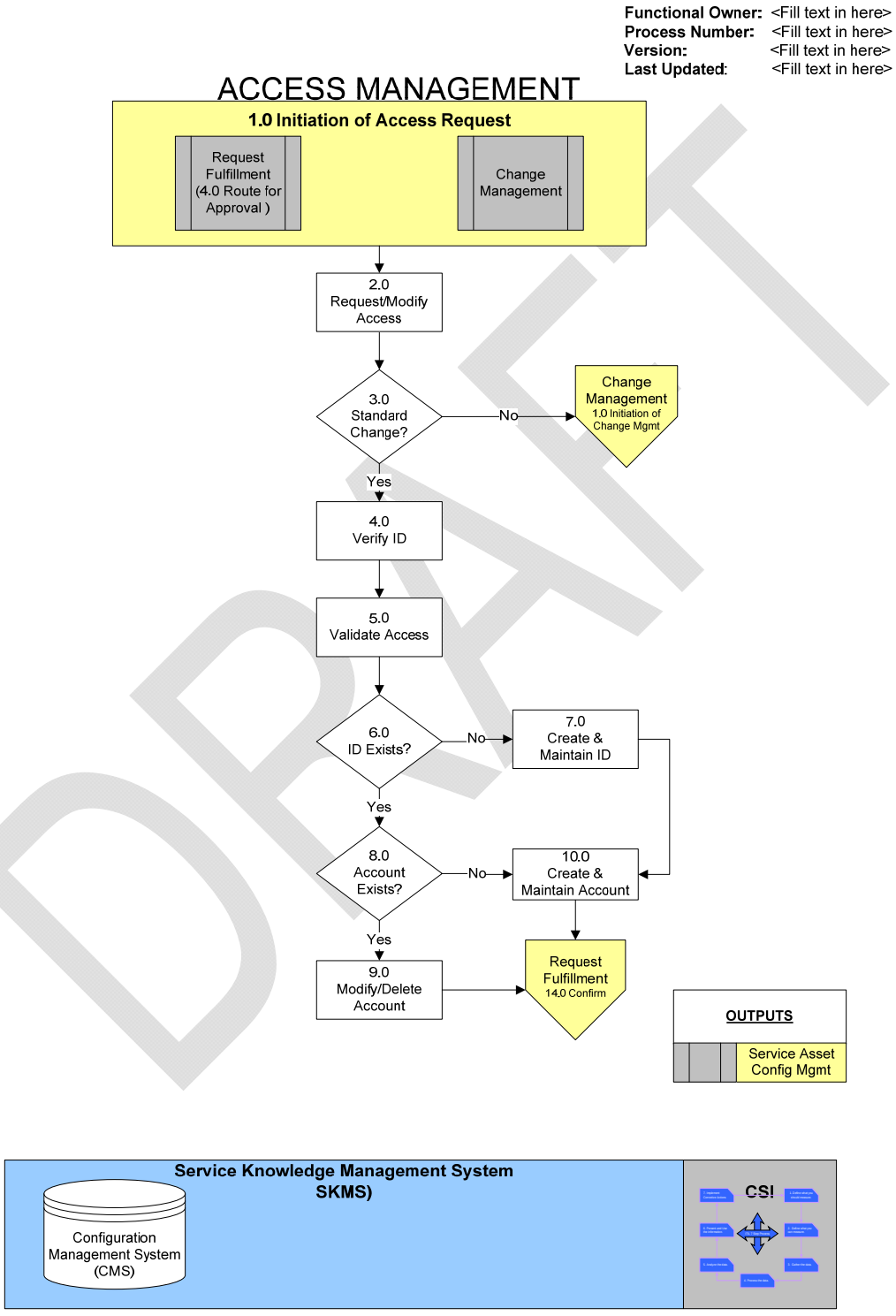


Figure 22 Access Management Model

5.3.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Initiation of Access Request	Assess all Access Requests through verification, providing rights, monitoring identity status, logging and tracking.
2.0	Request/Modify Access	Capture requests for access or changes to access privileges. Request changes for end-users as their responsibilities or employment status change.
3.0	Standard Change?	Determine the extent of the request. Does it qualify as a Standard Change or will it need to go through the Change Management process?
4.0	Verify ID	Validate identify of the person requesting access to a system.
5.0	Validate Access	Validate approval of the request. Provide Rights.
6.0	ID Exists?	Checks to determine if the user is already identified in the system.
7.0	Create and Maintain Account Create and maintain ID in the System	Issue/update CAC cards with user identification information.
8.0	Account Exists?	Checks to determine if the user has an active account in the system.
9.0	Modify/Delete Account	Monitor Identity Status and Maintain Users, Roles and Groups. Remove or Restrict Rights.
10.0	Create and Maintain ID? Create New Accounts?	Create new accounts for system access when they don't already exist.

5.3.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service

Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager	Service Provider Lead
	Ensure that Service personnel /subcontractors have the correct level of CAC access, physical access, account rights and clearance(s) to perform the required services.	CI	AR	R
	Conform to the Government requirements that justify needs for level of access.	CI	AR	R
	Conform to NGEN standards for granting access to each access level (e.g. requirement for changing passwords).	CI	AR	R
	Ensure that all personnel /subcontractors hold or are eligible to obtain the security clearance specified by the Government. At a minimum, personnel/subcontractors will be required to hold or have the ability to obtain a secret clearance.	CI	AR	R
	Use the Government's Contractor Verification System (CVS) for obtaining access to any Government system.	CI	AR	R

	Have a process in place to ensure that access rights are terminated or restricted upon death, resignation, dismissal, role change, and transfer or travel where different regional access applies (both system, network and physical).	CI	AR	R
	Ensure that Administrator access to a device is controlled to the degree that only authorized users can make changes to a device.	CI	AR	R
	Touch labor will ensure that Administrator access to a device is terminated when their work is complete.	CI	AR	R
	Have the ability to produce a report within one of business day that validates access privileges are relevant for all personnel/subcontractors.	CI	AR	R
	Provide the Government with system access to generate the following reports for each system or service: • Number of requests for access (Service Request, RFC, etc.) • Instances of access granted by service, user, departed, etc. • Instances of access granted by department or individual granting rights • Number of Incidents requiring a reset of access rights • Number of Incidents caused by incorrect access settings	CI	AR	R

5.3.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

Information Security Management

Availability Management

Capacity Management

Request Fulfillment

Service Level Management

Inputs

Consider the inputs to the process:

- Request for Fulfillment
- Policies from Security and Availability Management
- Change in Employee Status
- Request for Change
- Human Resource Management Event Notification (e.g. position changes, transfers, dismissals)

Outputs

Consider the outputs from the process:

- Access Request Fulfillment

5.3.6 Roles

The following roles have been identified with the process.

Roles	Description
Access Management Process Owner	This is the strategic role that is accountable for the Process.
Access Management Process Manager	This is the tactical role that performs cross-segment coordination and runs the day-to-day, end-to-end Process implementation activities.

5.3.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Define correct level of filtering of events and alerts	1	Number of Events and Alerts.
		2	Number of Events and Alerts that defined Incidents and Problems.
		3	Number of Events and Alerts caused by Known Errors.

2	Use appropriate tools for Event and Alert Monitoring supporting the automated monitoring of systems and services	4	Number of Events and Alerts that require human intervention.
		5	Number of Events and Alerts duplicated or repeated.
		6	Number of Events and Alerts that could be solved without human intervention.

5.3.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

Access/Identify Management Software

Configuration Management System (CMS)

Request Fulfillment Tracking System

Service Knowledge Management System (SKMS)

5.4 Incident Management

5.4.1 Process Overview

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within Service Level Agreement (SLA) limits.

5.4.2 High Level Process Model

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

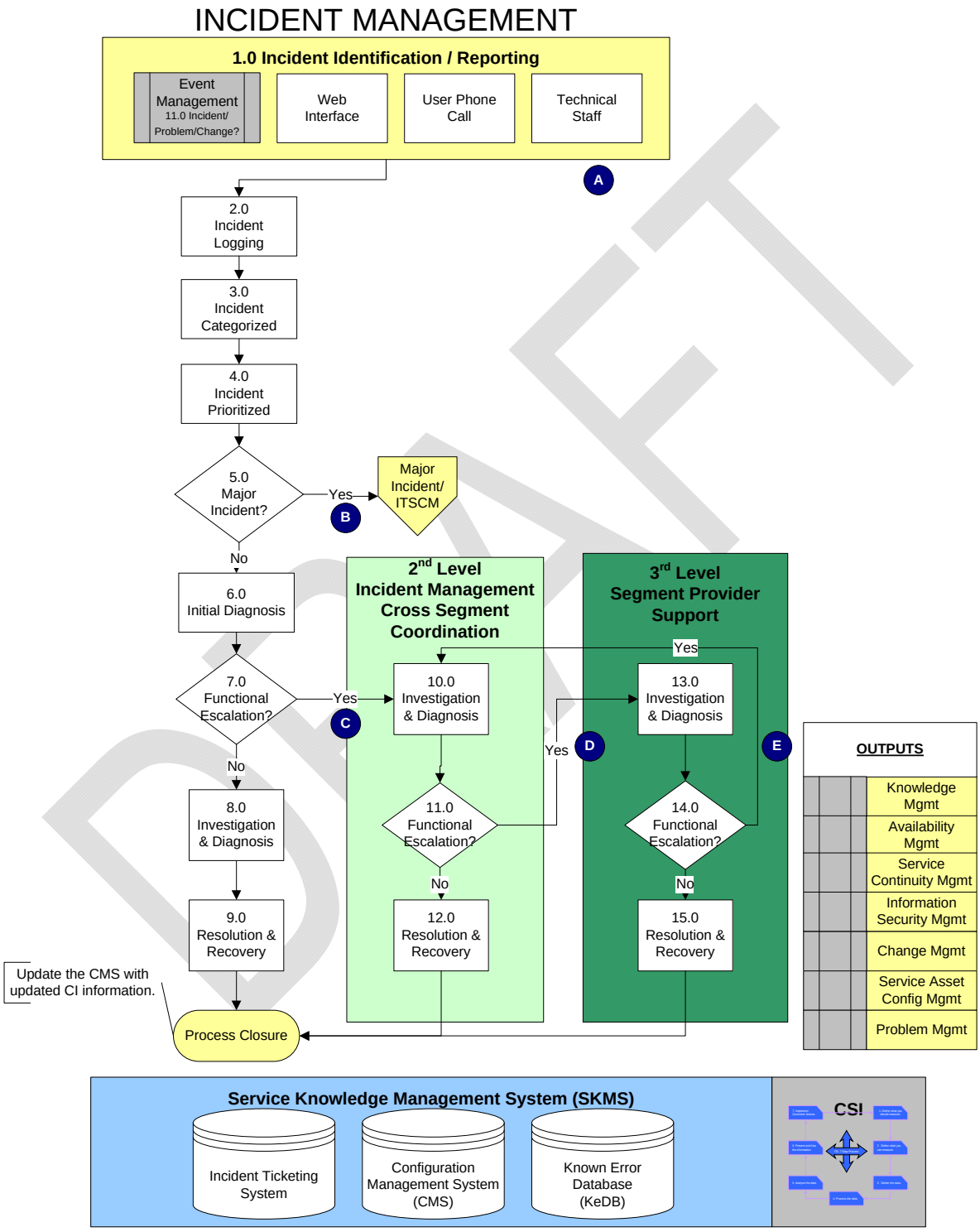


Figure 23 Incident Management Model

5.4.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Incident Identification & Reporting	There are multiple inputs that can identify and report an Incident. The items listed are examples of common methods of identifying and initiating the Incident Management process.
2.0	Incident Logging	The Incident is logged into the Incident tracking tool and an Incident ticket is created.
3.0	Incident Categorized	Incident is categorized based on the systems, applications or services/segment affected.
4.0	Incident Prioritized	The Incident is prioritized based on urgency and impact.
5.0	Major Incident	A key decision point to determine if the Incident meets the definition of a major Incident (high impact, high urgency Incident).
6.0	Initial Diagnosis	The Incident is diagnosed to discover the full extent of the symptoms, assess what has gone wrong and to try to resolve the issue.
7.0	Functional Escalation	This decision point is to determine if the issue can be resolved at this level of support or if it should be escalated to a specialist for further diagnosis.
8.0	Investigation and Diagnosis	In-depth investigation of the Incident looking for a resolution.
9.0	Resolution & Recovery	1st Level Resolution & Recovery. Service is restored using a solution / work-around. Recovery activities performed as required.
10.0	Investigation & Diagnosis	Upon escalation, the Second Level Support team will perform investigation and diagnosis of the Incident to determine effort required to address the Incident.
11.0	Functional Escalation	The 2nd Level Support team determines if this Incident needs to be escalated to a 3rd level support team (Segment). Note: this could involve multiple 3rd level support teams (segments). In this case the

		2nd level support team would be the coordinator of the Incident until it is resolved.
12.0	Resolution & Recovery	2nd Level activity. Service is restored using a solution / work-around. Recovery activities performed as required.
13.0	Investigation & Diagnosis	Upon escalation, the Third Level Support team will perform investigation and diagnosis of the Incident to determine effort required to address the Incident. The 3rd level support team will coordinate with 2nd level support as needed.
14.0	Functional Escalation	The 3rd Level Support team determines if this Incident needs to be escalated to one of the other 3rd level support teams.
15.0	Resolution & Recovery	3rd Level activity. Service is restored using a solution / work-around. Recovery activities performed as required. Coordination with the 2nd level of support as required.
	Incident Closure	Resolution confirmed with the customer or originator, Incident closed.
	Major Incident Process	There is a specific process for Major Incidents. This process will be initiated for all Incidents that meet, or appear to meet these criteria.

5.4.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
A	Identification/Reporting from Technical Staff to the Service Desk
B	Escalation from Service Desk to Major Incident Team (War Room)
C	Escalation from Service Desk to Government Owned 2nd Level team
D	Escalation from Government owned 2nd level team to the appropriate 3rd level support teams (includes Service Providers). This could result in a concurrent

	escalation to multiple organizations (including service providers).
E	Escalation from 3rd level support team back to the Government owned 2nd level team when additional teams need to be included in Incident resolution or the Incident was improperly assigned to the wrong 3rd level support team.

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager (Incident Manager)	Service Provider Lead
	Use or interface with the Government's Incident Tracking Tool to ensure there is a single source record for all Incidents.	CI	AR	R
	Have an Incident ticket tracking system capable of interfacing with the Government's Service Desk's Incident Tracking tool. Able to receive escalated Incident tickets, create new Incident tickets, update open Incident tickets and close Incident tickets assigned to them in real time.	CI	R	AR
	Support the use of a centralized Service Desk as the Users' first point of contact for reporting Incidents or system related issues (e.g. single toll-free number, single user-facing web interface, etc.).	CI	AR	R
	Notify the Service Desk and provide the appropriate information related to actions the Service Desk should take to minimize impact to Users (includes	CI	AR	R

	providing the Service Desk with the expected duration of the Incident and all other information the Service Desk requires to effectively support rapid Incident resolution)., upon becoming aware of an outage or Incident that impacts the Users of their service.			
	Provide resources for cross-segment Incident troubleshooting and resolution (coordinated by 2nd Level support).	CI	AR	R
	Accept and resolve all Incidents escalated to them (3rd Level) according to the defined Service Level Agreements.	CI	AR	R
	Maintain capability to respond to all escalated Incidents through the Government's Incident Tracking Tool.	CI	AR	R
	Shall not close an Incident Ticket until the Incident has been resolved to the satisfaction of the User. The Service Provider may close a resolved Incident after 5 days on a 24/7 basis if no response has been received from the User.	CI	AR	R
	Update and maintain Incident Tickets as each activity is performed (work log of actions). This would include, but is not limited to, change in status, troubleshooting steps, changes to settings, and handoffs to other personnel, etc.	CI	AR	R
	Provide information and appropriate training to the Service Desk sufficient to enable them to provide effective 1st and 2nd level support for the Service(s) provided. This would include documented information related to Known Errors, workarounds to common or reoccurring Incidents, known defects and the Configuration Management Database system.	CI	AR	R

	Adhere to the Government's Incident prioritization model, which is based on assessment of Urgency and Impact. The possible priorities are: 1 = critical, 2 = high, 3 = medium, 4 = low and 5 = planning. **IMPACT** **URGENCY** High: 1 / 2 / 3 Med: 2 / 3 / 4 Low: 3 / 4 / 5			
	Assist the Government in determining how to assess Urgency and Impact related to the Service(s) provided so that a correct priority can be determined when Incidents occur.	CI	AR	R
	Be prepared to meet SLAs in support of Level of Services (LOS) for DPD e.g. maintaining spares accessible to meet SLAs.	CI	AR	R
	Provide to the Government, and will assist in maintaining appropriate and sufficient Categories, Types and Items (CTIs) in the Incident Tracking Tool for each Service provided. These CTIs will enable effective escalations to the Service Provider and will also be required to generate Incident reports related to the Service(s).	CI	AR	R
	Work with the Government on the resolution of all hierarchical escalations. The Government (DON) will be the point of contact for all hierarchical escalations.	CI	AR	R
	Provide the following reports on a weekly basis in a format specified by the Government (the Government shall also have system access to generate these reports): • Detailed and Summary report on the ageing information for all open Incident Tickets including: • escalations	CI	AR	R

	• mitigations • completion dates • Detailed and Summary report on Mean time to resolve (MTTR) by Incident priority. • Detailed and Summary report of total Incidents resolved. • Detailed and Summary report on the Number of Incidents resolved by Customer grouping (e.g. Command, Site, etc.). • Detailed and Summary report on the number of Incidents reopened. • Detailed and Summary report on Incident by Category Type and Item (CTIs).			
	Conform with the recommended Service Level Agreement Criteria (SLAs). For example: • Incident Prioritization (based on Urgency and Impact): • Critical - Acknowledged within 5 min. Resolved within 1 hours on a 24/7 basis. • High - Acknowledged within 15 min. Resolved within 8 hours on a 24/7 basis. • Medium - Acknowledged within 1 hour. Resolved within 24 hours on a 24/7 basis. • Low - Acknowledged within 24 hours. Resolved within 48 hours. • Planning - Acknowledged within 24 hours. Resolved according to plan.			

5.4.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Event Management
- Problem Management

- Change Management
- Release and Deployment Management
- Service Level Management
- Configuration Management
- Knowledge Management

Inputs

Consider the inputs to the process:

- Customer Reports of Service Disruption
- Reports of Critical Incidents / Outages
- Event Alerts from Monitoring Tools
- Reports of Potential or Eminent Service Disruptions
- Forward Schedule of Change
- Release Schedule
- Service Level Agreements (SLA, OLA, UPC)
- Knowledge base / Known Error database
- Problems
- Configuration Management Database

Outputs

Consider the outputs from the process:

- Resolved Incident tickets
- Restored Service for Major or Critical Incidents
- Communications related to disruptions (during and after Incident)
- Post Incident Review
- Problem alerts
- Requests for Change (RFC)
- Documenting Incident resolution in the knowledgebase

5.4.6 Roles

The following roles have been identified with the process.

Roles	Description
Incident Manager	This role has the responsibility for producing or helping to produce management reports, managing the work of

	support staff, and typically acting as the Service Desk Manager by maintaining the Service Desk.

5.4.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Ability to resolve Incidents quickly	5	Incident Reopen Rate. NGEN will ensure that root causes of Incidents are identified and eliminated. Metrics will be developed, reported, and acted on. Calculated by Number of Incidents Reopened/ Total Number of Incidents. Threshold = <2%, Objective = <1%.
		6	Average Time to Resolve Severity Level 1 Incidents (Hours). Average response time to resolve severity 1 Incidents. Threshold = 24hrs, Objective = <8hrs.
		8	Incident Management Tooling Support Level. Assessment on the ability of the Incident management system toolset to support Incident management activities. NGEN will need to assess and report on how effective the existing tools are at addressing Incidents. Threshold = COBIT Maturity level 3, Objective = COBIT Maturity level 4.
2	Ability to maintain IT service quality	1	Number of Incident Occurrences. NGEN will need to assess and report on historical measurements for trending occurrences of Incidents. Calculated by Total Number of Incidents metrics. Threshold = Less than 100,000 (defects per million opportunities) dpmo (COBIT Maturity level 2) 2.78 process sigma, Objective = Less than 5,000 dpmo (COBIT Maturity level 3) 4.08 process sigma.
		2	Number of High Severity/Major Incidents. NGEN will need to use the Pareto principle to address the significant, relatively few high severity/major Incidents among the majority of the Incidents. Threshold = Less than 7,000 dpmo (COBIT maturity level 2) 3.96 sigma, Objective = Less than 1,000 dpmo (COBIT maturity level 3) 4.59 sigma.

		3	Incident Resolution Rate. NGEN will need to assess and report on how successful the system is at identifying and resolving issues. Calculated by Number of Incidents Resolved within Agreed Service Levels/ Total Number of Incidents.
		4	Customer Incident Impact Rate. NGEN will need to asses and report on how severely Incidents impact the customer experience. Severity level units are based on Failure Mode and Effect Analysis (FMEA) severity ratings. Threshold = severity level 6, Objective = severity level 2. Rate is calculated by Number of Incidents with Customer Impact/ Total Number of Incidents.
		8	Incident Management Tooling Support Level. Assessment on the ability of the Incident management system toolset to support Incident management activities. NGEN will need to assess and report on how effective the existing tools are at addressing Incidents. Threshold = COBIT Maturity level 3, Objective = COBIT Maturity level 4.
		9	Incident Management Process Maturity. Assessment on the ability of the Incident management process to execute Incident management activities. NGEN will need to asses and report on the overall effectiveness of the process. Threshold = COBIT Maturity level 3, Objective = COBIT Maturity level 4.
3	Ability to improve IT and customer productivity	7	Incident Labor Utilization Rate. NGEN will need to assess and report on how much available labor capacity is spent on addressing Incidents. Calculated by Total Labor Hours Spent Resolving Incidents (Non-Service Desk)/Total Available Labor Hours to Work on Incidents (Non-Service Desk). Threshold = 90%, Objective = 80%.
		8	Incident Labor Utilization Rate. NGEN will need to assess and report on how much available labor capacity is spent on addressing Incidents. Calculated by Total Labor Hours Spent Resolving Incidents (Non-Service Desk)/Total Available Labor Hours to Work on Incidents (Non-Service Desk). Threshold = 90%, Objective = 80%.
4	Ability to maintain user satisfaction	4	Customer Incident Impact Rate. NGEN will need to asses and report on how severely

			Incidents impact the customer experience. Severity level units are based on Failure Mode and Effect Analysis (FMEA) severity ratings. Threshold = severity level 6, Objective = severity level 2. Rate is calculated by Number of Incidents with Customer Impact/ Total Number of Incidents.
		8	Incident Management Tooling Support Level. Assessment on the ability of the Incident management system toolset to support Incident management activities. NGEN will need to assess and report on how effective the existing tools are at addressing Incidents. Threshold = COBIT Maturity level 3, Objective = COBIT Maturity level 4.
		9	Incident Management Process Maturity. Assessment on the ability of the Incident management process to execute Incident management activities. NGEN will need to asses and report on the overall effectiveness of the process. Threshold = COBIT Maturity level 3, Objective = COBIT Maturity level 4.

5.4.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Incident ticket tracking system capable of interfacing with the Service Desk's Incident Tracking tool. This must be able to receive escalated Incident tickets, create new Incident tickets, update open Incident tickets and close Incident tickets assigned to them in real time.
- Configuration Management System (CMS).

5.5 Problem Management

5.5.1 Process Overview

The goal of Problem Management is to minimize the adverse impact of Incidents and Problems on the business that is caused by errors within services and technology, and to prevent recurrence of Incidents related to these errors. In order to achieve this goal, Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.

The discovery and removal of errors in the infrastructure is the primary objective of Problem Management. The overall objective includes delivering the highest possible level of stability in IT services by finding and eliminating errors. It aims not only to minimize the impact of failures when these occur, but also, by using information accrued during Incident resolution, to correct the root causes of these failures and to request a change (RFC) to be put in place to permanently remove the errors. Problem Management achieves this by identifying the errors and removing them from the IT infrastructure.

A Problem is the unknown root cause of one or more existing or potential Incidents. Problems may sometimes be identified because of multiple Incidents that exhibit common symptoms. Problems can also be identified from a single significant Incident, indicative of a single error, for which the cause is unknown.

The DON is becoming more dependent on IT to achieve DON goals. Any disruption of service has an affect on the DON business. Ensuring that errors are removed from the IT infrastructure enables the DON to function at a required level. Problem Management provides a method and process to identify chronic issues and enable their elimination from the IT infrastructure with a structured approach. This increasing the availability and stability of IT services and allows DON to meet its mission.

The Problem Management process has both reactive and proactive aspects. The reactive aspect is concerned with solving Problems in response to one or more Incidents. Proactive Problem Management is concerned with identifying and solving Problems and Known Errors before Incidents occur in the first place.

5.5.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

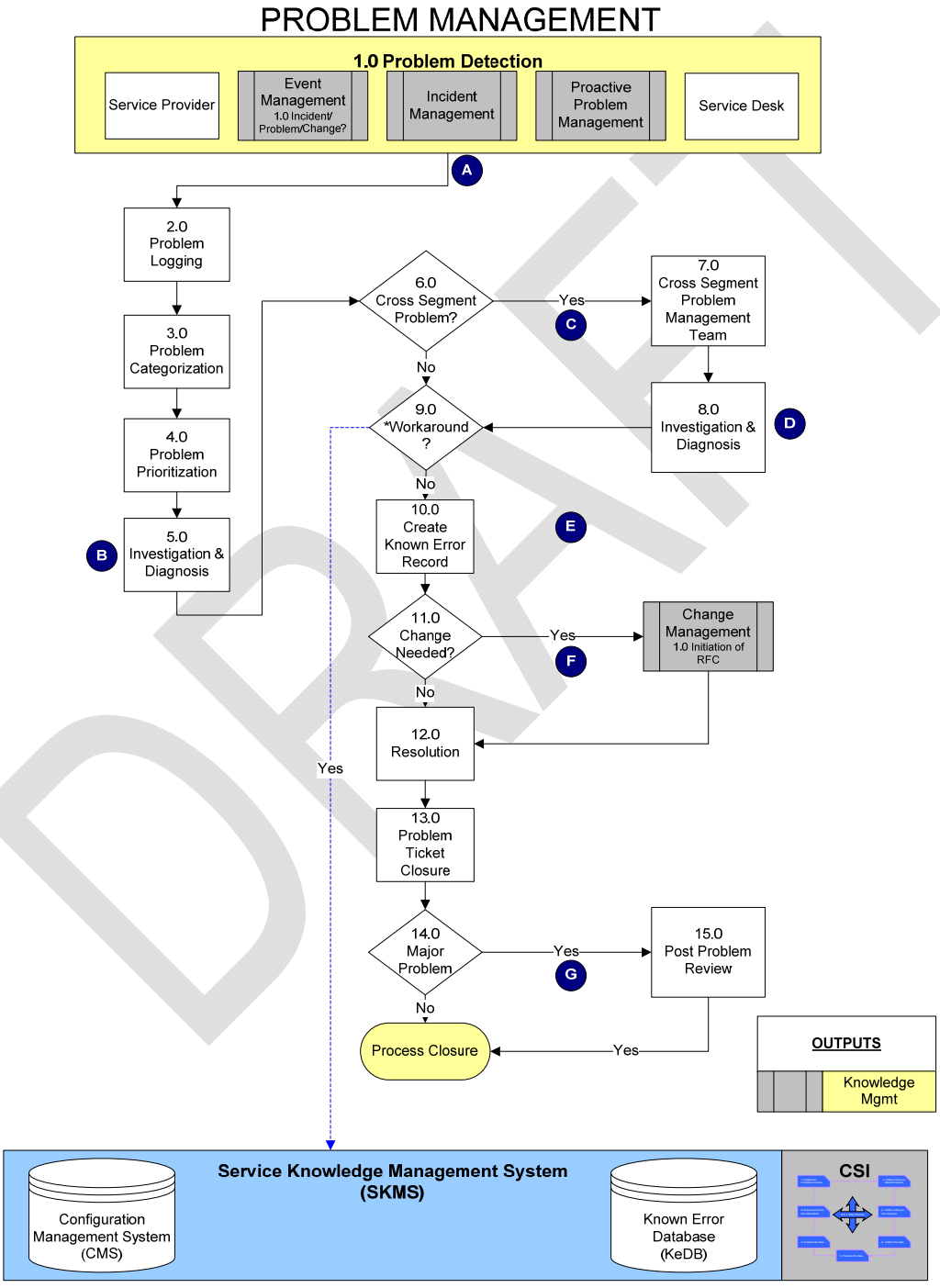


Figure 24 Problem Management Model

5.5.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
1.0	Problem Detection	Discovery of a Problem via alerts generated from Event Management, analysis by Incident Management, reports to the Service Desk, and notification from a Service Provider. Problem Management may also detect a Problem via analysis of Incident tickets.
2.0	Problem Logging	Problem Record in recorded in the Problem tracking tool detailing all relevant information. Problem record will be tracked and updated in Problem Tracking tool until closure.
3.0	Problem Categorization	Problem Record is categorized based on the systems, applications or services/segment affected (similar to Incident Management).
4.0	Problem Prioritization	Problem Record is prioritized based on urgency and impact (similar to Incident Management).
5.0	Investigation & Diagnosis	Use Problem solving techniques to identify the root cause of a Problem and determine requirements necessary to come to a permanent resolution of the Problem.
6.0	Cross-Segment Problem?	Determine whether the Problem involves more than one segment?
7.0	Cross-Segment Problem Mgt Team	Convene a high level Problem management team composed of representatives from relevant segments to mange and track cross-segment Problems.
8.0	Investigation & Diagnosis	Apply a methodical approach toward the identification of the root cause of the Problem while factoring in impact, severity and urgency considerations.
9.0	Workaround?	Determine whether there is a temporary method of circumventing the Problem. If there is a workaround to the issue, document the steps in the

		SKMS before proceeding. This allows Incident Management to address issues until a permanent fix is in place.
10.0	Create Known Error Record	Record the root cause as well as the workaround or permanent fix to a Problem in the Known Error Database (KeDB).
11.0	Change Needed?	Determine whether to raise and RFC to Change Management if the fix involves a change in functionality or interoperability.
12.0	Resolution	Apply the identified resolution to the Problem.
13.0	Problem Ticket Closure	Verify that the Problem has been corrected and close the Problem Record.
14.0	Major Problem?	Evaluate the Problem to determine if the Problem meets the criteria for a Post Problem Review.
15.0	Post Problem Review	Conduct a lesson learned session to capture efficiency and examine NGEN's response to the Problem.

5.5.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
A	Identification of a Problem by a Service Provider.
B	Validation of workaround by Problem Management team.
C	Determination of Cross Segment Involvement
D	Validation of workaround by Cross Segment Problem Management Team.
E	Creation and validation of Known Error record.
F	Assessment to determine change viability/feasibility.
G	Evaluation/Review

The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner	Process Manager (Problem Manager)	Service Provider Lead
	Assign a Problem Managers to monitor, track, report and ensure that Problem Management activities (e.g. root case analysis, recurring Incident analysis) are performed in accordance with SLA's.	CI	AR	R
	Uses interface with the Government's Problem Tracking Tool to ensure there is a single source record for all Problems. All Problems will be entered, updated and tracked in this single Tool.	CI	AR	R
	Work with the Government to evaluate cost and risk to determine if it is justifiable / feasible to implement a permanent fix to a known error (Problem).	CI	AR	R
	At the request of the Cross Segment Problem Management Team, the Service Provider shall provide resources to assist with the investigation, diagnosis and resolution of Problems that involve multiple segment providers.	CI	AR	R
	The Service Provider shall validate workarounds used by Incident Management (Service Desk) to resolve Incidents related to their service.	CI	AR	R
	The Service Provider shall populate the Knowledge Management system with the steps or procedures used to resolve Incidents and Problems (including all	CI	AR	R

	known errors and validated workarounds) as soon as the information is available. This information will be stored in the enterprise knowledge management system (SKMS).			
	When a change is required to resolve a known Problem, the Service Provider shall follow the enterprise Change Management process and shall contribute all deliverables necessary to obtain change management and release management permission to implement.	CI	AR	R
	The Service Provider shall assist the Government in appropriately determining how to assess "Urgency" and "Impact" related to the service(s) provided so that a correct priority can be determined when Problems are identified (e.g. the service provider will identify the criteria for the following priorities: critical, high, medium, low and planning).	CI	AR	R
	The Service Provider shall provide the Government and will assist in maintaining appropriate and sufficient Categories, Types and Items (CTIs) in the Problem Tracking tool for each service provided. These CTIs will enable effective assignments to the Service Provider(s) and will also be required to generate Problem reports related to the service(s).	CI	AR	R
	The Service Provider shall review Incident reports weekly to identify reoccurring Incidents related to their service that could be potential Problems.	CI	AR	R
	The Service Provider shall provide a weekly report containing the following information (the Government shall also have system access to generate these reports): • Total number of Problems attributable to the service provider and the number of Incidents associated with each Problem. • New Problems identified during the reporting period	CI	AR	R

	• Number of Problems that remain open • Total number of Problems where root cause analysis is complete and cause of the error is known. • A clear description of the cause and the requirements to permanently resolve the Problem shall be in the report. • The report will also indicate the considerations related to decision to implement or not implement a change to correct the Problem. • Detailed and summary reports of Problems closed during the reporting period. • Detailed and summary reports of Problems resulting in or attributed to a Request for Change (RFC). • Detailed and summary reports of Problems where an implemented change request failed to resolve the Problem. • Detailed and summary reports of knowledgebase articles entered that are associated with Incidents and Problems (this includes known errors and workarounds).			

5.5.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with the following ITSM processes:

- Incident Management
- Change Management
- Service Level Management
- Configuration Management
- Release and Deployment Management
- Knowledge Management
- Availability Management

- Capacity Management
- IT Service Continuity Management
- Financial Management

Inputs

Consider the inputs to the process:

- Event alerts or notices (system monitoring tools)
- Problem alerts
- Supplier or contractor notification
- Prioritization matrix priority standardization
- Incident Management trending reports
- Critical or Major Incident reports
- Configuration Details from the CMDB
- Workarounds documented in the knowledge base
- Known Error database
- Knowledge base trending reports
- Forward Schedule of Change

Outputs

Consider the outputs from the process:

- Known errors
- Validated workarounds
- Resolved Problems
- Identification of trends
- Proactive prevention of Problems and Incidents
- Updated Problem Records
- Requests for Change (RFC)
- Management information

5.5.6 Roles

The following roles have been identified with the process.

Roles	Description
Problem Management Process	The strategic role accountable for the process.

Owner	
Problem Management Process Manager (Problem Manager)	The tactical role responsible for cross-segment coordination.

5.5.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Ability to minimize the impact of Problems by reducing Incident frequency and duration	1	Incident Repeat Rate. NGEN will effectively ensure that Incidents are being analyzed for root cause. If true root causes of Problems are being eliminated the Incident repeat rate should be a critical metric that shows this. Calculated by Number of Repeat Incidents/ Total Number of Incidents. Threshold = <5% Incident repeat rate (50,000 dpmo, 3.14 sigma), Objective = <1% Incident Failure rate (10,000 dpmo, 3.83 sigma).
		2	Number of Major Problems. NGEN will need to assess and report on the major Problems (Pareto principle). How many occurred? Threshold = TBD, Objective = TBD).
		6	Customer Impact Rate. NGEN will need to asses and report on how customers are impacted by Problems. Calculated by Number of Problems with Customer Impact/ Total Number of Problems in Pipeline. Threshold = FMEA severity level 6, Objective = FMEA severity level 2.
		7	Average Problem Resolution Time. Problems will be addressed in a timely manner and customers informed of status. Calculated by Average Time to Resolve Problems – Severity 1 & 2 (Days). Threshold = 48hrs, Objective = <24hrs.
		9	Problem Management Tooling Support Level. NGEN will need to asses and report on how the current toolset supports Problem management activities. Threshold = Very Good, Objective = Excellent.

2	Ability to improve the quality of services being offered	1	Incident Repeat Rate. NGEN will effectively ensure that Incidents are being analyzed for root cause. If true root causes of Problems are being eliminated the Incident repeat rate should be a critical metric that shows this. Calculated by Number of Repeat Incidents/ Total Number of Incidents. Threshold = <5% Incident repeat rate (50,000 dpmo, 3.14 sigma), Objective = <1% Incident Failure rate (10,000 dpmo, 3.83 sigma).
		2	Number of Major Problems. NGEN will need to assess and report on the major Problems (Pareto principle). How many occurred? Threshold = TBD, Objective = TBD).
		10	Problem Management Process Maturity. Assess and report on how well Problem management activities are executed? Dashboard metrics will be developed using all the above mentioned critical success factors and supporting PAs. Threshold = Mature (<5%, 50,000 dpmo, 3.14 sigma) Or COBIT Maturity Model 2, Objective = Very mature (<.1%, 1,000 dpmo, 4.59 sigma) Or COBIT Maturity Model 3.5.
3	Ability to resolve Problems and errors efficiently and effectively	3	Problem Resolution Rate. Percentage of Problems that are eliminated. Calculated by Number of Problems Removed (Error Control)/ Total Number of Problems in Pipeline. Threshold = 95% baseline (50,000 dpmo, 3.14 sigma), Objective = 99% (10,000 dpmo, 3.83 sigma).
		4	Problem Workaround Rate. Assess and report on the percentage of Problems addressed by the implementation of workarounds. This is an important metric because workarounds often result in vulnerabilities in other areas of the system. Calculated by Number of Known Errors (Root Cause Known and Workaround in Place)/ Number of Repeat Incidents. Threshold = <5% Problem workaround rate (50,000 dpmo, 3.14 sigma), Objective = <1% Problem workaround rate (10,000 dpmo, 3.83 sigma).
		5	Problem Reopen Rate. Assess and report on if Problems are successfully removed permanently and, if so, to what degree of effectiveness. Calculated by Number of Known Errors (Root Cause Known and Workaround in Place)/ Total Number of

			Problems in Pipeline. Threshold = <5% Problem reopen rate (50,000 dpmo, 3.14 sigma), Objective = <1% Problem reopen rate (10,000 dpmo, 3.83 sigma).
		8	Problem Labor Utilization Rate. Assess and report on the available labor capacity that was spent handling Problems. Calculated by Total Labor Hours Spent Working on and Coordinating Problems/Total Available Labor Hours to Work on Problems. Threshold = 99%, Objective = 95%.
		9	Problem Management Tooling Support Level. NGEN will need to asses and report on how the current toolset supports Problem management activities. Threshold = Very Good, Objective = Excellent.
		10	Problem Management Process Maturity. Assess and report on how well Problem management activities are executed? Dashboard metrics will be developed using all the above mentioned critical success factors and supporting PAs. Threshold = Mature (<5%, 50,000 dpmo, 3.14 sigma) Or COBIT Maturity Model 2, Objective = Very mature (<.1%, 1,000 dpmo, 4.59 sigma) Or COBIT Maturity Model 3.5.

5.5.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Problem tracking tool that integrates or is compatible with the Incident Management ticket tool.
- Access to the enterprise knowledge management system and will be an active contributor and reviewer of knowledge and information.
- Access to the enterprise Change Management system to submit and monitor Requests for Change.
- Access to the Configuration Management system to identify system relationships and potential Problems.
- Access to Incident Management trending reports related to their service.

6 Continual Service Improvement

Continual Service Improvement (CSI) supports the importance of following a quality approach to improving service and embraces the importance of standards, especially ISO/IEC 20000-2005 (written prior to ITIL v3), which is the International Standard for certifying service provider organizations in IT Service.

CSI aims to define, identify and implement improvements to services, process, and infrastructure as well as measure, verify and report that these actions have been adequate, suitable, and effective. The CSI Manager and process are continually looking for ways to improve process efficiency and effectiveness as well as cost effectiveness in each stage of the lifecycle.

6.1 7-Step Improvement Process

6.1.1 Process Overview

The 7-Step Improvement Process is a key part of CSI which asks key questions about what to measure and where to find this information necessary to implement corrective action.

The key activities of the CSI element evolve around CSI's 7-step Improvement process. This process is similar in many ways to the Deming Cycle of Plan, Do, Check, Act (PDCA) and Six Sigma's Define, Measure, Analyze, Improve, Control (DMAIC). All established Quality Management and engineering methodologies should be considered in the improvement process; however the CSI 7-step process has 7 clearly defined steps.

In the context of this process, the overall goal should be to design and implement NGEN that creates end to end user satisfaction by using:

- ITIL standardization as the framework for ITSM
- Lean Six Sigma as the methodology to drive Continual Service Improvement, and create value and customer delight by eliminate deficiencies and waste using data driven approach
- ITIL Maturity Model to qualitatively and quantitatively measure quality of NGEN
- Extensive and comprehensive training to optimize effectiveness of NGEN operators in understanding and creating customer delight

CSI is dependent on top management's visible and voiced support. The process infrastructure must be planned, documented, implemented and verified through audit. The CSO process will also be dependent on ownership and continuity of process operators. Training and a clearly developed Body of knowledge for ITIL and especially CSI is also required.

6.1.2 High Level Process Model

The following diagram illustrates the high level process model.

Functional Owner: <Fill text in here>
Process Number: <Fill text in here>
Version: <Fill text in here>
Last Updated: <Fill text in here>

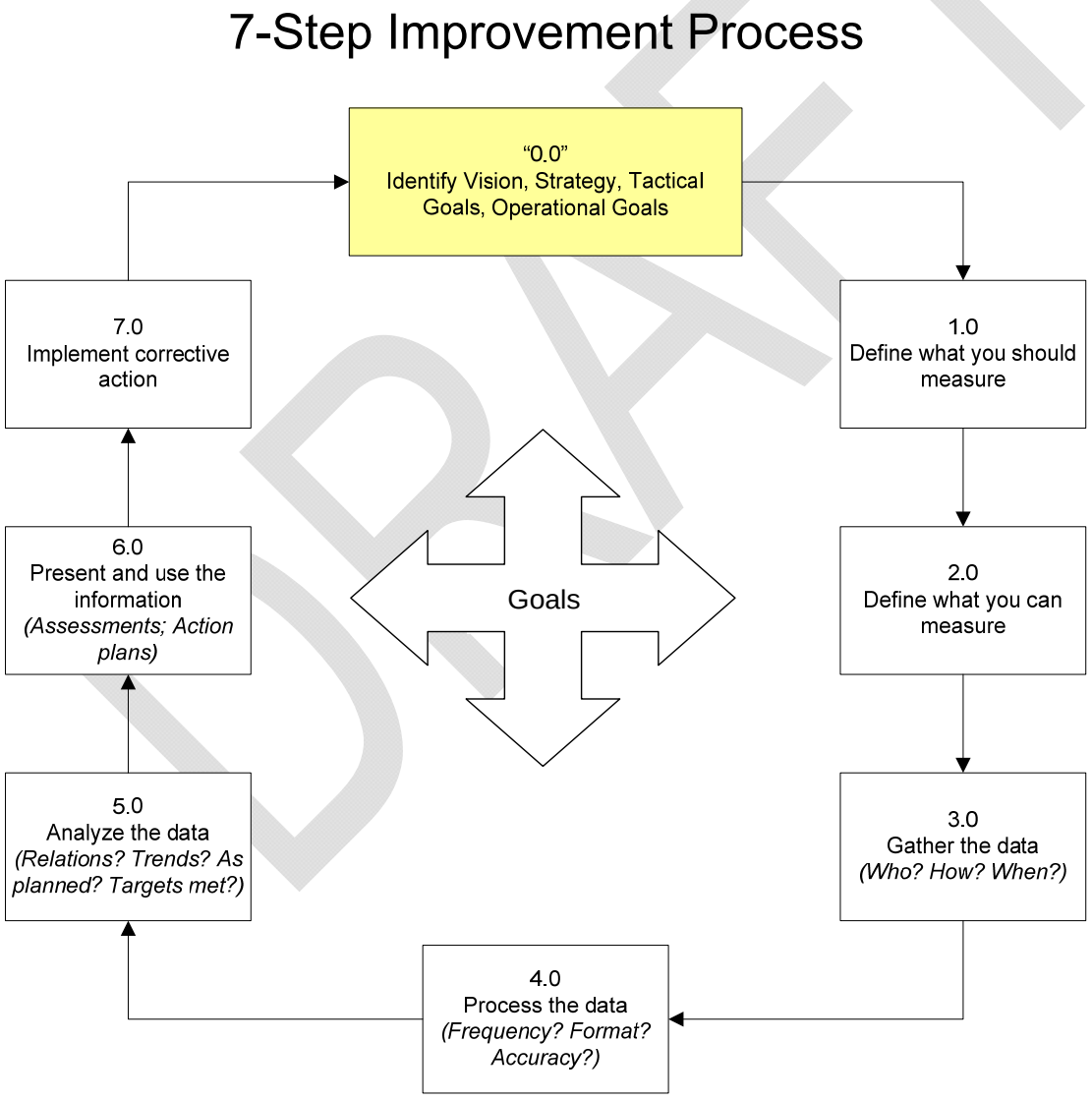


Figure 25 7-Step Improvement Process Model

6.1.3 High Level Process Descriptions

The sub-processes of the high level process model are described at a high level.

Number	Sub-process	Description
"0.0"	Identify Vision, Strategy, Tactical Goals, Operational Goals	Note that on-going activities include: • Continuously looking for ways to improve process efficiency and effectiveness • Continually looking for ways to improve cost effectiveness • Works to improve each stage of lifecycle (not just current services, people, and processes) • Benchmarking • Developing and maintaining a balanced scorecard • Knowledge management • Problem management • Process integration

1.0	Define what you should measure	Sources for measurement should include but not be limited to:
		• Any and all SLAs.
		• Critical processes identified by Service Lifecycle, Service Strategy, and Service Design.
		• What is critical to service:
		  • Critical to quality
		  • Critical to cost
		  • Critical to delivery.
		• What is the "voice of customer"?
		• What is the "voice of process"?
		• What is the "voice of business"?
		• Customer surveys.
		• Benchmarking results.
		• Lean Six Sigma black belt project selection and prioritization process.

		• Any policy, mission, goals, or objectives of the business. Compare to Lean Six Sigma: DEFINE
2.0	Define what you can measure	This stage is crucial as it serves as a toll gate for KPIs going forward. If it cannot be measured it should not be an SLA or KPI. This stage should also include what tools are in place or needed to measure the desired process or function. Compare to Lean Six Sigma: DEFINE
3.0	Gather the data	A process for gathering data should be developed for each measuring point. Technology metrics (component and application based metrics such as utilization, performance, and availability), process metrics (SLAs, KPIs, and activity metrics for the service management process), and service metrics (the results of end to end service) should be considered. Data gathering plans and activities should be based on collecting measurements that will serve to determine if CSI goals have been achieved. Data should also be gathered in a proactive "preventive" mindset to eliminate deficiencies and not just respond to them. Compare to Lean Six Sigma: MEASURE
4.0	Process the data	The data is gathered and put in required format(s). The gathered data should be analyzed to determine accuracy. This includes using gauge R&R, ANOVA, and other lean six sigma tools. Data should be matched with corresponding SLAs and KPIs. Compare to Lean Six Sigma: MEASURE
5.0	Analyze the data	This is the process of transforming data into information. Verification of actual results with goals and / or expected results is performed. This stage is critical for assuring that data presented to management is accurate. Gaps, trends and potential impact to business are assessed with data at this stage. Recommendations for corrective action and preferably preventive action are formulated at this stage. Compare to Lean Six Sigma: ANALYZE

6.0	Present and use the information	At this stage the information gathered from the other stages are presented and distributed to all critical and other interested parties (stakeholders). There are usually three distinct audiences: the business, senior IT management and internal IT with various interests. Data should be presented with attention given to target audience and associated goals and objectives of that audience. Data should be presented in a form that is specific to the audience and their needs. Compare to Lean Six Sigma: IMPROVE
7.0	Implement corrective action	This is where the knowledge gained is put to use on corrective and preventive actions as well as other improvement projects. Management should also review the overall efficiency of the 7-step process during this phase from time to time. If there are not the resources to implement all the recommended corrective and preventive actions management should establish priorities during this phase. Compare to Lean Six Sigma: CONTROL

6.1.4 Seam Management Authority Matrix

The term **seam** refers to a connection or interaction between one or more organizations. It could be an interaction between Government (DON) organizations, Government (DON) to IT Service Provider, or IT Service Provider to IT Service Provider. The seam analysis helps to identify the processes, people and technology required to coordinate end to end management of IT Services.

The following table provides key seam descriptions.

Seam	Seam Descriptions
	TBD

. The following tables identify key process activities and where possible, associate activity with process seams and key roles.

Seam	Required ITSM Process Specification
	N/A

The authority matrix below identifies process activities that can be associated with key roles and/or process seams. These relationships are documented in terms of RACI (Responsible, Accountable, Consulted, and Informed). This table does NOT represent a RACI mapping to the organization or sub-processes.

Seam	Required ITSM Process Specification	Process Owner (CSI Manager)	Process Manager (Service Owner)	Service Provider Lead
	Tools (meaning methods, not necessarily applications) for supporting CSI shall be developed as the process is implemented and matured. Many of the tools that need to be used in CSI are common the quality management and Lean Six Sigma. These include but are in no way limited to the following: • Assessment and gap analysis • Benchmarking • Balanced scorecards • SWOT analysis • Internal and 3rd party auditing • COBIT and / or CMMI • Quality Function Deployment (QFD) • 7 quality tools • 7 management tools • Failure Mode Effect Analysis (FMEA) • Design of Experiments (DOE) • Theory of Constraints (TOC) • Cost effective analysis			

6.1.5 Process Interfaces

Any process is triggered by an event or activity and associated artifact(s), and produces an output which typically feeds into another process.

Interfaces

This process has a key relationship or dependency with all ITSM processes.

Inputs

Consider the inputs to the process:

- Vision
- Strategy
- Tactical Goals
- Operational Goals
- Service Improvement Plan

- Service and process improvement needs
- Baseline assessments and gap analysis
- Measurement, data, metrics and targets
- Training
- Return on investment (ROI) and Cost effective analysis

Outputs

Consider the outputs from the process:

- Data, metrics, and other qualitative and quantitative data
- Service Improvement Plans
- Corrective and preventive actions
- Verifiable Voice of Customer and customer satisfaction
- Validated more efficient processes
- Improved customer and employee moral

Specific Six Sigma Outputs	Reference to Sub-processes
Well defined Problem statement List of process or product customers Input and output relationships (Y=f{X}) Metric trends (historical data) High level process map: supplier – input – process – output – customer (SIPOC) Project charter Project plan	Outputs from 1.0 and 2.0 (DEFINE)
Revised Problem statement and charter Detailed process map Cause and effect diagram followed optionally by Failure Mode and Effect Analysis (FMEA) Data collection plan Measurement system validation: gauge repeatability and reproducibility (R&R) Graphical analysis (7 quality tools) Baseline trend chart	Outputs from 3.0 and 4.0 (MEASURE)
Statistical analysis: Analysis of Variance (ANOVA), Design of Experiments (DOE), hypothesis testing Root cause per cause and effect diagram	Outputs from 5.0 (ANALYZE)

Understanding of process variation Refine improvement area Cycle time / Lead time Takt time (beat or rate time) Value Stream Map	
Statistical verification of variable list Potential solutions New process map Revised specifications (including upper control limit (UCL) and lower control limit (LCL) Revised FMEA New capability analysis and sigma level	Outputs from 6.0 (IMPROVE)
Error proofing Process documentation Control plans with reaction plans Trend charts verifying performance Internal audits External audits Value Stream Map	Outputs from 7.0 (CONTROL)

6.1.6 Roles

The following roles have been identified with the process.

Roles	Description
CSI Manager (Process Owner)	This role represents the CSI process owner and is ultimately responsible and accountable for the success of all improvement activities, ensuring that best practice is adopted and sustained throughout the organization.
Service Owner (Process Manager)	This role represents a CSI process manager and is accountable for a specific service. This role is responsible for seeing that the CSI process is implemented and maintained throughout their organizations.
Service Manager	This role manages the development, implementation, evaluations and on-going management of new and existing products and services.
Reporting Analyst	This role reviews and analyzes data from components, systems, and subsystems in order to obtain an end-to-end

	service achievement

6.1.7 Performance Metrics

The effectiveness and performance of the process are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators
1	Improve IT Service Quality.	1	Increased rate of customer satisfaction ratings in restoring service.
		2	Increased rate of customer perception of service support.
2	Reduce IT Costs.	1	Reduced costs in technical assets
		2	Cost of improvement effort

6.1.8 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further development of the process:

- Incident Management
- Problem Management
- Asset and Configuration Management

For the quality and management tools referenced above, personnel trained in Six Sigma, ITIL, and other quality and IT disciplines shall be required. Other automated data collections tools shall be designed into the internet system as required. These tools should be identified as early in the process as possible. Design for Six Sigma should be deployed at the onset of the process in order to better engineer tools for collecting and reporting data.

6.2 Service Measurement

6.2.1 Process Overview

Create and build a business-focused service-reporting framework, including the definition and agreement to policy and rules for service design and how it will be measured, assessed and reported (including recommended actions for prevention, correction and improvement). These actions and activities include but are not limited to the following:

- Targeted audience and related business views
- Identification and agreement on what is to be measured and reported on (metrics)
- Defined and agreed upon scope of activities

- Basis of all calculations
- Reporting schedules and distribution
- Access to reports and medium to be used
- Meetings scheduled to review and discuss results including the establishment and agreement of actions and a plan for following up to see that the actions were carried out and were effective.

6.3 Service Reporting

6.3.1 Process Overview

IT must be able to measure against an end-to-end service. Effective reporting extends beyond snapshots of adherence to service level agreements. It should show trends of past performance, including impacts and related solutions, as well as current and forecasted status and improvement efforts.

For services there are three basic measurements:

- Availability of service
- Reliability of service
- Performance of service

The following tasks need to be performed for service level measurement:

- Develop service management framework
- Define the different levels of measurement and reporting
- Define what is to be measured
- Set targets
- Determine service process level measurements
- Create measurement framework grid
- Interpret and use metrics
- Use measurement and metrics
- Create scorecards and reports
- Enforce policies and governance
- Auditing the effectiveness of planned measurements and systems

7 IT Service Management Functions

The term *function* in the context of an organization is a logical concept referring to the people and automated measures that carry out tasks and activities defined by processes and procedures. In larger organizations a function may be broken up and performed by several departments, teams or groups, or it may be embodied within a single organizational unit.

7.1 Service Desk

7.1.1 Function Overview

The Service Desk is the primary point of contact for users to experiencing a service disruption or wishing to request a service or a change. This function has dedicated staff members who deal with service events that alert them by phone, monitors or web interfaces.

7.1.2 Roles

The following roles have been identified with the function.

Roles	Description
Service Desk Manager	This customer-services role manages key service desk activities and roles including supervisors, serving as an escalation point, reporting business-impacting issues, attending CAB meetings and taking accountability for Incidents and service requests.
Service Desk Supervisors	This role focuses on the staffing, skill level and shifts of the support personnel, assists the Service Desk Manager as needed, produces reports, arranges training, and liaises with other key service management staff during changes, deployments and overall support.
Service Desk Analysts	This role provides first-level support, handling Incidents and service requests.

7.1.3 Key Activities

The Service Desk will be NGEN users' first point of contact and first level of support for (at least) Incident Management. Consider the following key activities associated with a Service Desk.

The Service Desk creates the request ticket and fulfills the request if possible. If it is unable to do so, the ticket is assigned to the appropriate, specialized team. The Service Desk uses all available resources and knowledge tools to resolve as many issues as possible at the first level. Any issues that cannot be addressed within defined SLAs will be escalated the appropriate second or Nth level support team for resolution.

All customer contact with the Service Desk, whether it is request fulfillment, complaints or Incident reports, will be tracked in a tool. All vendors who participate in the Service Desk function, Incident Management, Problem Management or Request Fulfillment processes need to use the same or compatible tool or have the ability to communicate with it in real-time.

All Service Level Agreements applicable to the Service Desk are tracked, monitored and reported using the guidelines and format designated by the Government. Typical measurements are:

- First call resolution
- First level resolution
- Average time to resolve an issue
- Average speed of answer or response to contact with the Service Desk
- Average time to escalate an issue to other levels of support
- Call abandonment rates

The Service Desk offers end users multiple options for obtaining assistance based on Government requirements. Examples of methods of contact are typically phone, voice mail, fax, e-mail, web chat, self-help.

The Service Desk owns all Request Fulfillment tickets and Incident tickets and will be responsible to follow-up on tickets that do not meet SLAs.

The Service Desk is responsible for assessing all reported Incidents. Using an established priority model, the Service Desk analysts effectively assess the urgency and impact of the issue and assign the appropriate priority for the Incident. This would include VIP and Major Incident identification.

The criteria for establishing priorities for Incidents and requests will be understood and followed consistently by all Service Desk Analysts.

Hours for operations for the Service desk along with other Service Level Agreements are defined by the Government's Service Level Manager.

The Service Desk uses and populates an enterprise knowledge management process and tool to assist in providing consistent, quality resolution to Incidents, Problems, questions and requests.

The Service Desk is responsible for training new Service Desk analysts but can call upon the assistance of other NGEN subject matter experts as needed.

Customer satisfaction surveys are used to assess overall satisfaction with the Service Desk function and IT services.

The effectiveness and performance of the function are measured using metrics-based Key Performance Indicators (KPIs) which support high level Critical Success Factors (CSFs). The CSFs and KPIs below are examples which may or may not reflect actual Key Performance Parameters (KPPs).

CSF #	Critical Success Factors	KPI #	Key Performance Indicators

1	Resolve Customer Issues on First Call	1	Service Desk Call Resolution Rate.
		3	Service Desk Tooling Support Level.
2	Maintain Customer Productivity	1	Service Desk Call Resolution Rate.
		3	Service Desk Tooling Support Level.
		6	Call Duration Experience.
3	Provide a Positive Customer Call Experience	3	Service Desk Tooling Support Level.
		5	Call Abandon Rate.
		6	Call Duration Experience.
		7	Call Waiting Rate.
		8	Service Desk Service Availability.
4	Provide Effective Support for Customer Calls	3	Service Desk Tooling Support Level.
		4	Call Agent Utilization.

7.1.4 Tools Interface Requirements

The following known tool interfaces requirements should be considered during further organization of the function:

- Service desk or CRM tool
- Knowledgebase tools
- Configuration Management tool
- Request Fulfillment tool
- E-mail system
- Phone ACD system
- Web site for self-service, self-help and communication

7.2 Technical Management

7.2.1 Function Overview

Technical Management refers to the groups, departments or teams that provide technical expertise and overall management of the IT infrastructure. Technical management also plays an important role in the design, testing, release and improvement of IT services. It may also be responsible for the daily operation of a subset of the IT infrastructure.

This function is the custodian of technical knowledge an expertise related to managing the IT infrastructure and ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and refined. It provides the actual resources to support the ITSM lifecycle. In this role Technical Management ensures that resources are effectively trained and deployed to design, build, transition, operate, and improve the technology required to deliver and support IT Services.

7.2.2 Roles

The following roles have been identified with the function.

Roles	Description
Technical manager/ Team Leader	This role provides overall leadership and control of an infrastructure-specific team.
Technical Analysts/ Technical Architects	This role is a staff member who performs technical activities focused on user needs, technical design, operating systems, and infrastructure.
Technical Operator	This role carries out day-to-day operational activities for the infrastructure, which are similar to IT Operations staff.

7.2.3 Key Activities

The Technical Management function carries out generic tasks, including the following:

- Identifying knowledge expertise required to manage and operate the IT Infrastructure.
- Initiating training programs.
- Recruiting or contracting resources with the skills that cannot be developed internally or where resources are needed.
- Defining or establishing standards used in the design of new architectures.
- Carrying out research and development of solutions that can expand the Service Portfolio.
- Participating in the design and build of new services.

The following departments represent typical, specialized technical teams:

- Mainframe team
- Server team
- Storage team
- Network support team
- Desktop team
- Database team

- Middleware team
- Directory Services team
- Internet or web design team
- Messaging team
- IP-based Telephony

7.2.4 Tools Interface Requirements

Tool interfaces requirements cannot be specified in any detail as IT infrastructure is so broad.

7.3 IT Operations Management

7.3.1 Function Overview

IT Operations is the department, group or team of people responsible for performing the organization's day-to-day operational activities such as running the production line in a manufacturing environment or managing the distribution centers and fleet movements within a logistics organization. IT Operations is the function responsible for ongoing management and maintenance of an organization's IT Infrastructure to ensure delivery of the agreed level of IT service to the business.

7.3.2 Roles

The following roles have been identified with the function.

Roles	Description
IT Operations Manager	This role provides overall leadership and control of IT Operations.
Shift Leaders	This role provides leadership during the shift period, ensuring that operational activities are running well, and managing Operations Analysts.
IT Operations Analysts	This role is a senior IT Operations staff focusing on in-depth technical proficiencies and operational efficiencies.
IT Operations	This role carries out day-to-day operational activities, such as installations, backups, and housekeeping.

7.3.3 Key Activities

The IT Operations Management function carries out generic tasks, including the following:

- Operations Control which oversees the execution and monitoring of the operational activities.
- Job scheduling.

- Backup and restore.
- Print and output management.
- Maintenance activities.
- Facilities Management.

7.3.4 Tools Interface Requirements

Tool interfaces requirements cannot be specified in any detail as IT operations and facilities management are so broad.

7.4 Application Management

7.4.1 Function Overview

Application management is responsible for managing applications throughout their lifecycle. The application management function is performed by a group or team involved in managing and supporting operational applications. It also plays an important role in the design, testing, and improvement of applications that form part of IT Services.

Application management is to applications what Technical Management is to the IT Infrastructure. Application Management plays a role in all applications whether purchased or developed in-house.

7.4.2 Roles

The following roles have been identified with the function.

Roles	Description
Application Managers/ Team Leaders	This role is dedicated to one application, taking responsibility for leadership of the team, providing technical knowledge, ensuring necessary training, and communicating with users.
Application Analysts/ Architect	This role is responsible for matching business requirements to system or application specifications.

7.4.3 Key Activities

One key set of activities associated with Application Management is the custodianship of technical knowledge and expertise related to managing applications. In this role, Application Management working together with Technical Management ensures that the knowledge required to design, test, manage and improve IT services is identified, developed and maintained.

Another key set of activities involves the provision of resources to support the ITSM Lifecycle. In this role, Application Management ensures that resources are effectively trained and deployed to design, build, and transition, operate and improve the technology required to deliver and support IT services.

7.4.4 Tools Interface Requirements

Tool interfaces requirements cannot be specified in any detail as they depend on the business applications in question.

Appendix A Revision History Archive

This table of revision history predates the information in the Document Control section.

Version	Date	Author	Group	Change
0.01	05-07-08	Scott Hales, Buck Stearns, Tony Funkhouser		Pulled information from the ITIL Process Definitions document to create v1.0 of this Process Interface Document. The purposed of this information is to be an input into the NGEN RFP/SOW work.
0.02	06-03-08	ITSM COE and SS West		Integrated the ITIL requirements at the Service Provider segment Level (Desktop and Peripherals) segment)
0.03	06-16-08	ITSM COE and SS West		Defined ITIL requirements for all Service Operations Processes to obtain Review Board feedback on appropriate level of detail for the SS and approach to defining the Seams. Answers the questions: who, what, when.
0.04	06-30-08	ITSM COE		Completed definition of ITIL requirements for all Service Operations and Service Transition Processes, at a level designed to be generically applicable to all segments. (Assume each segment SME team will tailor the requirements for its specific segment.). The team is evaluating how to best define the ITIL requirements for the Service Strategy and Service Design Processes, as these materially differ in nature from the "Operational" Processes defined thus far.
0.05	07-14-08	ITSM COE		Completed Service Design Processes as well as Service Portfolio Management.
0.06	07-18-08	ITSM COE		Completed Service Strategy. Updated and normalized entire document.
0.07	07-29-08	ITSM COE		Document edited, baseline and sent out for comment review.
0.08	07-31-08	ITSM COE		Changed order of diagrams and definition pages. Other general format changes.
0.09	09-05-08	ITSM COE		Change document name to ITIL Process Interface Document and Incorporated NETOPS comments.
0.10	09-17-08	SS Design Team		Made changes to various sections changing

				the 'TBD' to the actual owner. These changes were simultaneously made in the SS document 'Appendix E'. Added 'Document Identification Number' identification to 1st and every page following guidance from the Library Management Process Guide (LMPG). Change version numbering per the LMPG.
0.11	10-06-08	SS Design Team		Global replace 'NGEN PMO > NGEN PM' and made the following changes per the SS effort Appendix E updates: - pg 11 (Service Portfolio Management), bullets 2, 3, 4, 5, 9, 10, 11 and 12 - pg 19 (Financial Management), bullets 1, 2, 3, 4, and 8 {deleted 9 & 10) - pg 26 (Demand Management), bullets 1 and 5 (deleted bullet 7) under roles following changes from SS Appendix E. #7 stated: 'The Government (DON) will identify opportunities to optimize demand (reduce spikes in demands and incentives to mold the PBA). - pg 40 (Service Level Management), bullets 2 and 5 (deleted bullet 1) - pg 47 (Supplier Management), bullets 1 (deleted 'assisted by service deliver IPT) - pg 61 (Availability Management), bullet 2 under roles following changes from SS Appendix E. - pg 66 (IT Service Continuity Management), bullet 2 (deleted bullet 1) - pg 76 (Information Security Management), bullet 2 (deleted bullet 1) - pg 92 (Change Management), bullet 2 (deleted bullet 1) - pg 92 (Asst and Configuration Management), bullet 2 (deleted bullet 1) - pg 110 (Release and Deployment Management), bullet 2 and 3 (deleted bullet 1) - pg 127 (Service Validation and Testing), bullet 2 (deleted Service Validation & Testing IPT) - pg 127 (Service Validation and Testing), bullet 2 (deleted Service Validation & Testing IPT) - pg 134 (Knowledge Management), bullet 2 (deleted bullet 1) - pg 144 (Event Management), bullet 2 (deleted bullet 1) - pg 151 (Incident Management), bullet 2 (deleted bullet 1) - pg 167 (Problem Management), bullet 2

				(deleted bullet 1) Based upon updated direction from CDR McNeal resulting from the 10/8/08 RACI meeting the following changes were made: Service Level Management Replace Content with: 1. NNWC and MCNOSC, as Process Manager, will monitor and manage Service Provider's SLA compliance with PM NGEN Services Delivery team supporting. This is the tactical role that performs cross-segment coordination and ensures that all Service Catalog SLAs are monitored, analyzed and reported on, and changed or modified as required. Replace Content with: 2. PM NGEN will be the Process Owner of the Service Level Management Process. This is the strategic role that is accountable for the Service Level Management Process. Reversed Order of #1 and #2. Begin section with PM NGEN will be the Process owner…. Change Management: Replace Content with:1. PM NGEN will be the Process Owner and Manager for NGEN's Change Management Process. These are the strategic and the tactical roles that perform cross-segment coordination and run the day-to-day, end-to-end Process implementation activities. Ensures that Process is implemented in a standardized and repeatable manner. Asset and Configuration Management: Replace Content with:1. PM NGEN will be the Process Owner and Manager for NGEN's Asset and Configuration Management Process. These are the strategic and the tactical roles that perform cross-segment coordination and run the day-to-day, end-to-end Process implementation activities. Ensures that Process is implemented in a standardized and repeatable manner. The Process Manager will rely heavily on the Enterprise Services

				segment. Knowledge Management: Replace Content and break out into two sentences as follows: 1.PM NGEN will be the Process Owner for NGEN's Knowledge Management Process. This is the strategic role accountable for the Knowledge Management Process. 2. NNWC and MCNOSC will share the role of Process Manager for NGEN's Knowledge Management Process. This is the tactical role that performs cross-segment coordination and runs the day-to-day, end-to-end Process implementation activities. Ensures that Process is implemented in a standardized and repeatable manner. The Process Manager will rely heavily on the Enterprise Services segment. (i.e. managing and adding information to the SKMS, recommending changes to the existing content etc). Request Fulfillment: Replace Content with: NETOPS & MCNOSC will be the Process Owner of the Request Fulfillment Process. This is the strategic role and is accountable for the Process. Replace Content with: NETOPS & MCNOSC will be the Process Manager of the Request Fulfillment Process. This is the tactical role that performs cross-segment coordination and runs the day-to-day, end-to-end Process implementation activities. It ensures that the Process is implemented in a standardized and repeatable manner. Availability Management: Replace Content with:2. NETOPS & MCNOSC will be the Process Owner of the Access Management Process. This is the strategic role and is accountable for the Process.
0.12	11-12-08	Louis Ronzitti		Various changes following 'Composite Stakeholder Review Comments' (v0.13). Changes also transcribed into v1.14 of the 'NGEN Service Design Specification'.
0.13	11-17-08	Louis Ronzitti		Accepted all changes from v0.12.
0.14	11-20-08	Louis Ronzitti		Changed format of document. Made various editorial changes to conform to new format. Added content as it applies to new

				categories. Created Assumptions and Risks section. Added Glossary and Acronym listing.
0.15	11-24-08	Louis Ronzitti		Updated content for many of the new sections added after v0.14 included the 'Strategy Generation' process.
0.16	11-20-08	Louis Ronzitti		Added 'Request Fulfillment' process. Updated 'Strategy Generation', Global replacement 'Government' to 'DON', editorial changes in format throughout, Roles updated per CDR McNeal input.
0.17	12-01-08	Louis Ronzitti		Added content for Inputs/Outputs. Corrected previous global replace in References section (changed DON to Government). Added Functions, Continual Service Improvement and Service Measurement. Fixed format on sub-bullets. Added content (Overview, Objectives) to various processes.
0.18	12-10-08	Louis Ronzitti		Updated roles for the following processes: SLM, Capacity Management, ITSCM, ISM, Service Evaluation, Service Validation & Testing and Problem Management. Replaced SPO with ACNO NGEN and SDS with SS. Added additional terms to Glossary and Acronyms. Added comments from 'Composite Stakeholder Review Comments' (v0.19). Specifically, substantive tab ITSM 016 – ITSM 144 and administrative ITSM 36 – ITSM 50.
0.19	12-15-08	Louis Ronzitti		Updated Incident Management table with correct steps. Added updated flow charts from the 'Process Interface Document Flows.vsd' version 0.06. Flows updated included (but not limited to) Capacity Management, Release & Deployment Management, Event Management, Incident Management, Problem Management and Request Fulfillment. Added content for some CSF and KPIs.
0.20	01-12-09	Louis Ronzitti		Updated incorrect table numbering throughout document. Added tables for capturing seam information. Added definition of a 'seam' to the Glossary. Deleted sixth bullet (redundant to fourth bullet) under section 7.4.10. Updated table 16 to reflect 'seam' work done. Since this is a WIP, this table approach is still under review. The update only provided for

				illustration purposes. Updated Header/Footer information, Table of Contents and Table of Figures. Updated Service Desk; Definition, Function Overview and Objective, CSFs and KPIs. Added Service Catalog Management; CSFs/KPIs, Supplier Management; KPIs (for CSF2), Process Overview, Objective, Inputs, Outputs and KPIs, Release and Deployment Management; CSFs and KPIs, Service Evaluation; Management Process Overview, Objective and Relationships, Service Validation and Testing; CSFs and KPIs, Knowledge Management; Process Overview, Objective, Relationships, CSFs and KPIs, Event Management; CSFs and KPIs, Incident Management; CSFs and KPIs, Request Fulfillment; CSFs and KPIs, Access Management; CSFs and KPIs. Change para 4.1.3.1 from DON owned and DON operated to Government owned and Government operated. Change para 5.1.5.1 from '…these reports…' to '…Availability Reports…'. Deleted 'The assumption is that' from para 4.1.6.1.
0.21	02-18-09	Louis Ronzitti		Updated CSF/KPIs for Event Management, Supplier Management, and Financial Management processes. Added missing NGEN Roles (Service Provider) section to Information Security Management. Minor corrections throughout following Administrative comments from the 'Composite Stakeholder Review Comments' v0.39 spreadsheet as part of the Block 1 Increment 1 Service Specification Stakeholder Review. Since information from Appendix E of that document was provided from the PID, the comments made are synchronized. Added Service Level Management Flow from 'Process Interface Document Flows' v0.06.
0.22	02-20-09	Louis Ronzitti		Added new tables for Roles. This was done for the Capacity Management Process only. If the decision to use this approach is approved, then these tables should be replicated for all processes. If the decision is to not use this approach, revert to v0.21 for the previous Roles format.
0.23	03-06-09	Ashley Amjad		Basic spelling check and quality review

				prior to redesign and new content.

Appendix B Abbreviations

Abbreviation	Term
AAUSN	Assistant for Administration to the Under Secretary of the Navy
ACAT	Acquisition Category
ACD	Automatic Call Distribution
ACE	Advanced Computing Environment
ACL	Access Control List
AD	Active Directory
ADL	Advanced Distance Learning
ADNS	Automated Digital Network System
AIS	Automated Information Systems
AIT	Automated Information Technology
AKO	Army Knowledge Online
ALSP	Acquisition Logistics Support Plan
AM	Availability Management
AMHS	Automated Message Handling System
AMIS	Availability Management Information System
AoA	Analysis of Alternatives
API	Application Programming Interface
APL	Allowance Parts List
APM	Assistant Program Manager
APML	Acquisition Program Manager Logistics Assistant Program Manager for Logistics

APS	Application Service Provider
AS	Acquisition Strategy
ASD(NII)	Assistant Secretary of Defense for Networks & Information Integration
ASN	Applications, Servers and (Network Operating Centers) NOCs
ASN RDA	Assistant Secretary of the Navy for Research, Development and Acquisition
ASP	Application Service Provider
AS-SIP	Assured Services Session Initiation Protocol
ASTM	American Society for Testing and Materials
ATO	Approval to Operate
AV	All View
B1	Boundary One
B2	Boundary Two
B3	Boundary Three
BAN	Base Area Network
BCA	Business Case Analysis
BCM	Business Capacity Management Business Continuity Management
BCP	Business Continuity Plan
BER	Bit Error Rate
BIA	Business Impact Analysis
BIC	Battlefield Information Center
BLII	Base Level Information Infrastructure
BOIP	Basis of Issue Plan
BOM	Bill of Material

BPM	Business Processes Management/Modeling
BPMN	Business Process Modeling Notation
BRM	Business Relationship Management
BSM	Business Service Management
BUMED	Bureau of Medicine and Surgery
BW	Bandwidth
C&A	Certification and Accreditation
C2	Command and Control
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers & Intelligence
CAB/EC	Change Advisory Board / Emergency Committee
CAC	Call Admission Control Common Access Card
CAIV	Cost as an Independent Variable
CAL	Assurance Category Assignments List
CANES	Consolidated Afloat Network Enterprise Services
CAO	Competency Aligned Organization
CAR	Cyber-Asset Reduction
CARD	Cost Analysis Requirements Document
CARS	Cyber Asset Reduction and Security
CAT	Category
CBA	Capabilities Based Analysis
CBM	Conditioned-Based Maintenance
CBRN	Chemical, Biological, Radiological, and Nuclear

CBSP	Commercial Broadband Satellite Program
CBT	Computer-Based Training
CCE	Common Computing Environment
CCIE	Cisco Certified Internetwork Expert
CCM	Component Capacity Management
CDD	Capability Development Document
CDR	Critical Design Review
CDRLs	Contract Delivery Requirements Lists
CDS	Cross Domain Security
CENTRIXS	Combined Enterprise Regional Information Exchange System
CEO	Center of Excellence
CERT	Computer Emergency Response Team
CES	Core Enterprise Services
CFIA	Component Failure Impact Analysis
CHENG	Chief Engineer
CHINFO	Navy Chief Information Officer
CI	Configuration Item
CIE	Common Information Environment Controlled Information Exchange
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRT	Computer Incident Response Team
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction

CLIN	Contract Line Identification Number
CLS	Contractor Logistics Support
CM	Configuration Management Content Management
CMC	Commandant of the Marine Corps
CMDB	Configuration Management Database
CMS	Configuration Management System
CMIS	Capacity Management Information System
CMMI	Capability Maturity Model Integration
CMP	Configuration Management Plan
CMS	Configuration Management System
CNA	Center for Naval Analysis
CNA	Computer Network Attack
CND	Computer Network Defense
CND RA	Computer Network Defense Response Actions
CNE	Computer Network Exploitation
CNIC	Commander, Navy Installations Command
cNNPI	Classified NNPI
CNO	Chief of Naval Operations Computer Network Operations
COA	Course of Action
COBIT	Control Objectives for Information and Related Technologies
CO-CO	Commercially Owned - Commercially Operated
COE	Center of Excellence
COI	Community of Interest

COI JEC	Community of Interest Joint Evaluation Committee
COMMARFOR	Commander of Marine Forces
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations (Plan)
COP	Common Operating Picture
COTS	Commercial off the Shelf
CPD	Capability Production Document
CPI	Critical Program Information
CPIC	Capital Planning and Investment Control
CRAS	Classified Remote Access Service
CRL	Certificate Revocation List
CROP	Common Relevant Operational Picture
CRS	Computer Resources Support
CSA	Configuration Status Accounting
CSF	Critical Success Factor
CSI	Continual Service Improvement
CSP	Core Service Package
CTI	Computer Telephony Integration
CTIs	Categories, Types and Items
CVS	Contractor Verification System
DA	Decision Agent
DAA	Designated Approval Authority
DAG	Defense Acquisition Guidebook

DAU	Defense Acquisition University
DBMS	Data Base Management System
DCO	Deputy Commanding Officer
DD	DoD Form Declaration Document
DDG	Guided Missile Destroyer
DDMS	DoD Discovery Metadata Specification
DFARS	Defense Federal Acquisition Regulation Supplement
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
DIACAP	DOD Information Assurance Certification and Accreditation Process
DiD	Defense-in-Depth
DiffServ	Differential Services
DIICOE	Defense Information Infrastructure Common Operating Environment
DIKW	Data-to-Information-to-Knowledge-to-Wisdom
DISA	Defense Information Systems Agency
DISA JIEO	DISA Joint Interoperability and Engineering Organization
DISA NCES	Defense Information Systems Agency Net-Centric Enterprise Services
DISN	Defense Information Systems Network
DISR	DoD Information Technology and Standards and Profile Registry
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DKO	Defense Knowledge Online
DML	Definitive Media Library
DMS	Defense Messaging System

DMSMS	Diminishing Manufacturing Sources And Material Shortages
DMZ	Demilitarized Zone (Computing)
DNS	Director, Navy Staff
DNS	Domain Name Service
DoD	Department of Defense
DoD ESI	Department of Defense Enterprise Software Initiative
DoDAF	DoD Architectural Framework
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DON	Department of the Navy
DON ESI	Department of the Navy Enterprise Software Initiative
DON IM/IT	Department of the Navy Information Management/Information Technology
DoT	Department of Transportation
DOTMLPF	Doctrine, Organization, Training, Material, Leadership, Personnel, and Facilities
DPD	Desktops, Peripherals, and Devices
DPMO	Defects per million opportunities
DRCM	Detection and Reporting Category Matrix
DREN	Defense Research and Engineering Network
DRMO	Defense Reutilization and Marketing Office
DRR	Design Readiness Review
DRSN	Defense Red Switch Network
DS1	Digital Signal 1carrier signaling scheme
DSA	Defense Acquisition Strategy

DSCP	Differential Services Code Points
DSN	Defense Switch Network
E3	Electronic Effects Environment Electromagnetic Environmental Effects
EA	Electronic Attack
EAE	Enterprise Architecture Environment
EAG	Enterprise Action Group Enterprise Advisory Group
EAI	Enterprise Applications Integration
EC	Enabling Construct (e.g. CJCS, Applications Enabling Construct, 1 November 2005. Appendix F of the NCOE JIC.)
ECAB	Emergency Change Advisory Board
ECCB	Executive Configuration Control Board
ECDN	Enterprise Content Delivery Network
ECP	Engineering Change Proposals
ECS	Environment Control Service
E-DMZ	Enterprise Demilitarized Zone (Computing)
EDR	Engineering Design Reviews
EDS	Electronic Data Systems Corporation
EIE	Enterprise Information Environment
EIRs	Engineering Improvement Recommendations
EIS	Enterprise Information Systems
EITC	Enterprise Information Technology Support Center
EITSC	Enterprise IT Support Center
EM	Enterprise Management

EMIO	Extended Maritime Intercept Operation
EMP	Electromagnetic Pulse
EMRLS	Engineering and Manufacturing Levels
EPF	Enterprise Portal Framework
EPM	Enterprise Performance Management
ERP	Enterprise Resource Planning
ES	Electronic Warfare Support
eSCK-SP	eSourcing Capability Model for Service Providers
eSCM-CL	eSourcing Capability Model for Client Organizations
ESD	Electronic Software Distribution
ESDE	Enterprise Services & Data Environment
ESDS	Electrostatic Discharge Sensitive
ESG	Executive Steering Group
ESH	Enterprise Software and Hardware Environmental Safety Health
ESM	Enterprise Services Management
ESOH	Environment, Safety, and Occupational Health
ESOH	Environment Safety and Occupational Health
ETA	Early Transition Activity
ETJ	Electronic Training Jackets
EVM	Earned Value Management
EW	Electronic Warfare
FA	Functional Assessment
FAA	Functional Area Analysis

FAM	Functional Area Manager
FBICDs	Functional Baseline Interface Control Documents
FCA	Functional Configuration Audit
FCAPS	Fault, Configuration, Accounting, Performance, Security
FFC	Fleet Forces Command
FFP	Firm Fixed Price
FISMA	Federal Information Security Management (Act of 2002)
FITT	Fleet Integration and Transition Team
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects Criticality Analysis
FNA	Functional Needs Analysis Functional Needs Assessment
FOC	Full Operational Capability
FoS	Family of Systems
FRACAS	Failure Reporting and Corrective Action System
FRDC	Function Responsibility Decision Criteria
FSA	Functional Solutions Analysis
FSC	Forward Schedule of Changes
FTA	Fault Tree Analysis
FTS	Federal Telecommunications System
FW	Firewall
FY	Fiscal Year
GAL	Global Address List
GCCS	Global Command and Control System

GDS	Global Directory Services
GES	GIG Enterprise Services
GETS	Government Emergency Telecommunications System
GFE	Government Furnished Equipment
GIG	Global Information Grid
GIG BE	Global Information Grid Bandwidth Expansion
GIG CES	Global Information Grid Core Enterprise Services
GIG ES	Global Information Grid Enterprise Services
GNO	Global Network Operations
GNOC	Global Network Operations Center
GNOSC	Global Network Operations and Security Center
GO-CO	Government Owned - Commercially Operated
GO-GO	Government Owned - Government Operated
GOTS	Government Off-the-Shelf
GPETE	General Purpose Electronic Test Equipment
GUI	Graphical User Interface
HAIPE	High Assurance Internet Protocol Encryptor
HAZMAT	Hazardous Materials
HDML	Hand-held Device Markup Language
HEMP	High-Altitude Electromagnetic Pulse
HERF	Hazardous Emission of Radiation to Fuel
HERO	Hazardous Emissions of Radiation to Ordnance
HERP	Hazardous Emission of Radiation to Personnel
HFE	Human Factors Engineering

HIRF	High Intensity Radio Frequency
HMX	Marine Helicopter Squadron
HQMC	Headquarters Marine Corps
HQMC P&R	Headquarters Marine Corps Programs and Resources
HSI	Human System Integration
HSIP	HSI Plan
HTML	HyperText Markup Language
HW	Hardware
IA	Information Assurance
IAS	Information Assurance Strategy
IATC	Initial Authorization To Connect
IATO	Interim Approval to Operate Initial Authorization To Operate
IATT	Initial Authorization To Test
IAVA	Information Assurance Vulnerability Alert
ICAPS	Interactive Computer Aided Provisioning System
ICD	Interface Control Document Initial Capability Document
ICT	Information Communications Technology
ICW	Interactive Courseware
IDS	Intrusion Detection System
IETM	Interactive Electronic Technical Manual
IG	Inspector General
ILA	Integrated Logistics Assessment
ILS	Integrated Logistics Support/Sustainment

IM	Information Management
IMS	Integrated Master Schedule
INO	IT-21/NMCI/ONE-NET
IO	Information Operations
IO CTA	Information Operations Capstone Threat Assessment
IOC	Initial Operational Capability Initial Operational Capacity
IP	Intellectual Property Internet Protocol
IPS	Intrusion Prevention System
IPT	Integrated Product Team
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISEA	In-Service Engineering Agent
ISG	IT Steering Group
ISM	Information Security Management
ISMS	Information Security Management System
ISNS	Integrated Ship Networking System
ISO	International Organization for Standardization
ISP	Internet Service Provider Information Support Plan
ISSP	Information System Security Policy
IT	Information Technology
IT-21	Information Technology for the 21st Century (US Navy IT program to improve shipboard communications and computing capability)

ITC	Information Technology Center
ITIL	Information Technology Infrastructure Library
ITSCM	Information Technology Service Continuity Management
ITSM	Information Technology Service Management
ITU-T	International Telecommunication Union – Telecommunication
IVR	Interactive Voice Response
IW	Information Warfare
JAEC	Joint Assessment and Enabling Capability
JCDE	Joint Concept Development and Experimentation
JCIDS	Joint Capabilities Integration and Development System
JEDS	Joint Enterprise Directory Service
JFC	Joint Functional Concepts
JIC	Joint Integrating Concept
JIEO	Joint Interoperability and Engineering Organization (DISA)
JKDDC	Joint Knowledge Development and Distribution Capability
JNTC	Joint National Training Capability
JTA	Joint Technical Architecture Job Task Analysis
JTF COI	Joint Task Force Community of Interest
JTF GNO	Joint Task Force Global Network Operations
JTIC	Joint Interoperability Testing Command
JTRS	Joint Tactical Radio System
JV	Joint Vision
KEDB	Known Error Database

KIPS	Key Interface Profiles
KMDB	Knowledge Management Database
KPI	Key Performance Indicator
KPP	Key Performance Parameter
KSA	Key System Attribute Key Service Attribute
LAN	Local Area Network
LCCE	Life-Cycle Cost Estimates
LCE	Life-Cycle Engineering
LCM	Life-Cycle Management
LCMS	Learning Content Management Systems
LDAP	Lightweight Directory Access Protocol
LMI	Logistics Management Information
LNC	Legacy Network Consolidation
LORA	Level of Repair Analysis
LOS	Levels of Service
LRA	Local Registration Authority
LRFS	Logistics Requirements Funding Summary
LRU	Lowest Replaceable Unit
LSA	Logistics Support Analysis
LWG IPT	Logistics Working Group Integrated Product Team
MAC	Mandatory Access Control Mission Assurance Category Move-Add-Change
MAGTF	Marine Air Ground Task Force

MAIS	Major Automated Information Systems
MAN	Metropolitan Area Network
MANPRINT	Manpower and Personnel Integration
MARCERT	Marine Corps Computer Emergency Response Team
MARCORSYSCOM	Marine Corps Systems Command
MARFORCOM	Marine Corps Forces Command
MARFORRES	Marine Corps Forces Reserve
MB	Megabyte
MBPS	Megabits per Second
MC	Maintenance Concept
MCAS	Marine Corps Air Station
MCBQ	Marine Corps Base Quantico
MCEBJFP	Military Communications Electronics Board Joint Frequency Panel
MCEITS	Marine Corps Enterprise Information Technology Services
MCEN	Marine Corps Enterprise Network
MCGNOSC	Marine Corps Global Network Operations and Security Center
MCI	Marine Corps Installation
MCM	Management Control System
MCNOSC	Marine Corps Network Operations and Security Center
MCRC	Marine Corps Recruiting Command
MCTN	Marine Corps Tactical Network
MD	Management Domain
MDA	Maritime Domain Awareness
MDR	Metadata Repository

ME	Manpower Estimate
MESC	Maintenance Engineering Support Center
MHQ/MOC	Maritime Headquarters/Maritime Operations Center
MILCON	Military Construction
MilDet	Military Detachment
MILSPEC	Military Specification
MIL-STD	Military Standard
MILSTRAP	Military Standard Transaction Reporting And Accounting Procedures
MILSTRIP	Military Standard Requisitioning And Issue Procedures
MITSC	MAGTF Information Technology Support Center
MITSC	Marine Corps Information Technology Security Center
MLPP	Multilevel Precedence and Preemption
MLS	Multilevel Security
MML	Mobile Markup Language
MNIS	Multinational Information Sharing
MOA	Memorandum of Agreement
MOC	MCEITS Operation Center
MOSA	Modular Open Systems Approach
MOU	Memorandum of Understanding
MPLS	Multi-Protocol Label Switching
MPT&E	Manpower, Personnel, Training and Education
MRL	Material Requirements List
MSDS	Material Safety Data Sheet
MSGBn	Marine Corps Security Guard Battalion

MTBF	Mean Time Between Failures
MTBSI	Mean Time Between Service Incidents
MTRS	Mean Time to Restore Service
MTTR	Mean Time to Resolve/Recovery
MTU	Maximum Transmission Unit
MWOs	Modification Work Orders
N6	Office of the Deputy Chief of Naval Operations for Communications Networks
NAC	Network Access Control
NAVAIR	Naval Air Systems Command
NAVCIRT	Navy Computer Incident Response Team
NAVFAC	Naval Facilities Engineering Command
NAVGNOSC	Navy Global Network Operations and Security Center
NAVRESOR	Naval Reserve Forces Command
NAVSEA	Naval Sea Systems Command
NAVSTA	Naval Station
NAVSUP	Naval Supply Systems Command
NCCP	Net Centric-Capabilities Pilot
NCE	Net-Centric Environment
NCE JFC	Net-Centric Environment Joint Functional Concept
NCES	Net-Centric Enterprise Services
NCIS	Naval Criminal Investigative Service
NCOE JIC	Net-Centric Operational Environment Joint Integrating Concept
NCOW	Net-Centric Operations and Warfare
NCOW RM	Net-Centric Operations and Warfare Reference Model

NCTAMS	Navy Computer and Telecommunications Area Master Station
NCTS	Navy Computer and Telecommunications Station
NCW	Net-Centric Warfare
ND	Network Defense
NDIs	Non-Developmental Items
NECC	Net-Enabled Command Capability
NEO	Noncombatant Evacuation Operation
NEP	Network Equipment Provider
NEPA	National Environmental Policy Act
NESI	Net-Centric Enterprise Solutions for Interoperability
NET	New Equipment Training
NETC	Naval Education and Training Command
NETCOP	Network Common Operational Picture
NETOPS	Network Operations
NETWARCOM	Naval Network Warfare Command
NGEN	Next Generation Enterprise Network
NGEN TF	Next Generation Enterprise Network Task Force
NGO	Non-government Organization
NII	Networks and Information Integration
NIPRNET	Non-Classified Internet Protocol Router Network
NITSC	Navy Information Technology Support Center
NKO	Navy Knowledge Online
NM	Network Management
NMCI	Navy Marine Corps Intranet

NMIC	National Maritime Intelligence Center
NMS	Network Management System
NNE	Naval Networks Environment
NNPI	Naval Nuclear Propulsion Information
NNSOC	Naval Network and Space Operations Command
NNWC	Naval Network Warfare Command
NOAA	The National Oceanic Atmospheric Administration
NOC	Network Operations Center
NR	Net-Ready
NREMS	Navy Regional Enterprise Messaging System
NR-KPP	Net-ready Key Performance Profiles
NR-KPP-DD	Net-ready Key Performance Profiles (NR-KPP) Declaration Document
NSA	National Security Agency
NSERC	Naval Systems Engineering Resource Center
NSR	Network Service Representative
NSS	National Security System
NSWC	Naval Surface Warfare Command
NTOPS	New Technologies for Office and Portable Systems
NTP	Network Time Protocol
NTSP	Naval Training System Plans
NV	Network Visibility
O&M	Operations and Maintenance
OA	Operational Availability
OAAT	Open Architecture Assessment Tool

OAG	Operational Advisory Group
OCONUS	Outside the Continental United States
OCP	Oracle Certified Professional
ODAA	Operational Designated Approving Authority
OEM	Original Equipment Manufacturer
OJT	On-the-job Training
OLA	Operational Level Agreement
ONE-NET	OCONUS Navy Enterprise Network
ONI	Office of Naval Intelligence
ONR	Office of Naval Research
OPCON	Operational Control
OPEVAL	Operational Evaluation
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Office of the Chief of Naval Operations Instruction
OPSEC	Operational Security
OS	Operating Systems Open System
OSA	Open System Architecture
OSD	Office of the Secretary of Defense
OSI	Open Systems Interconnection
OT&E	Operational Testing and Evaluation
OV	Operational View
OWA	Outlook Web Access
P&G	Policy and Governance

PAC	Pacific
PACFLT	Pacific Fleet Command
PACOM	United States Pacific Command
PART	Program Assessment and Review Tool
PBA	Performance-Based Agreements Pattern of Business Activity
PBAS	Precedence-Based Assured Services
PBBE	Performance Based Business Environment
PBL	Performance-Based Logistics
PC	Personal Computer
PCA	Physical Configuration Audit
PDA	Personal Digital Assistant
PDR	Preliminary Design Review
PEO	Program Executive Office
PEO C4	Program Executive Office Command, Control, Communications, and Computers
PEO C4I	Program Executive Office Command, Control, Communications, Computers & Intelligence
PEO EIS	Program Executive Office for Enterprise Information Systems
PEP	Performance Enhancing Proxies
PESHE	Programmatic Environment, Safety, and Occupational Health Evaluation
PET	Performance Evaluation Tool
PFS	Prerequisite for Success
PHS&T	Packaging, Handling, Storage, and Transportation
PID	Process Interface Document

	Project Initiation Document
PIR	Post Implementation Review
PKI	Public Key Infrastructure
PM	Program Manager
PMM	Protocol Management Module
POA&M	Plan of Action and Milestones
POC	Point-of-Contact
POM	Program Objective Memorandum
POP	Point of Presence
POR	Program of Record
POTS	Plain Old Telephone Service
PPBE	Performance-Based Business Environment
PPS	Ports, Protocols, and Services
PSI	Physical Site Identifier Product Support Integrator
PSN	Packet Switched Networks
PSO	Projected Service Outage
PSTN	Public Switched Telephone Network
Py-EP	Policy Enforcement Points
QA	Quality Assurance
QDR	Quadrennial Defense Review
QMS	Quality Management System
QoS	Quality of Service
R&D	Research and Development
R&M	Reliability and Maintainability

RACI-VS	Responsible, Accountable, Consulted, Informed, Verified, Signed Off
RAM	Reliability, Availability, and Maintainability
RBAC	Role-Based Access Controls
RBS	Readiness-Based Sparing
RCA	Root Cause Analysis
RCM	Reliability Centered Maintenance
RDBMS	Relational Database Management System
RDT&E	Research, Development, Test and Evaluation
RED	Random Early Detection
RFC	Request for Change Request for Comment
RFID	Radio Frequency Identification
RFP	Request for Proposal
RFW	Radio Frequency Weapon
RM	Reference Model
RMA	Return Material Authority
RMC	Regional Maintenance Center
RNOSC	Regional Network Operations and Services Commands
ROI	Return on Investment
RPO	Recovery Point Objective
RSP	Remedy Skilled Professional
RTO	Recovery Time Objective
RTS	Real-Time Services
SA	Supportability Analysis Situational Awareness

SaaS	Software-as-a-Service
SAC	Service Acceptance Criteria
SACM	Service Asset and Configuration Management
SAMP	Single Acquisition Management Plan
SAN	Storage Area Networks
SATCOM	Satellite Communications
SCD	Supplier and Contract Database
SCM	Service Capacity Management
SDPs	Service Delivery Points
SDS	Service Design Specification
SE	Support Equipment
SE&I	Systems Engineering and Integration
SEAPRINT	System Engineering and Personnel Integration
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SEP	Support Equipment Plan
SETR	System Engineering Technical Review (SPAWAR).
SFA	Service Failure Analysis
SIM	Serialized Item Management
SIPRNET	Secret Internet Protocol Router Network
SKMS	Service Knowledge Management System
SLA	Service Level Agreement
SLM	Service Level Management
SLP	Service Level Package

SLR	Service Level Requirement
SMART	Specific, Measurable, Achievable, Relevant, Timely
SME	Subject Matter Expert
SMF	Service Management Function
SOA	Service-Oriented Architecture
SOC	Security Operation Center
SOP	Standard Operating Procedures
SOR	Statement of Requirements
SoS	Source of Supply System of Systems
SOW	Statement of Work
SPAWAR	Space and Naval Warfare Systems Command
SPAWARINSTs	Space and Naval Warfare Instructions
SPETE	Special Purpose Electronic Test Equipment
SPI	Service Provider Interface
SPM	Service Portfolio Management
SPO	System Program Office Service Provisioning Optimization
SPOF	Single Point of Failure
SRR	Services Requirements Review
SSA	Systems Security Authorization Software Support Activity
SSAA	Super-Sampling Anti-Aliasing System Security Authorization Agreement
SSL	Secure Sockets Layer

SSO	Single-Sign On
SSP	Safety System Plan
STEP	Standardized Tactical Entry Point
STIG	Security Technical Implementation Guidelines
SV	System View
SW	Software
SWAP	Size, Weight and Power
T&E	Test and Evaluation
TA	Technical Authority
TACON	Tactical Control
TAG	Technical Advisory Group
TAS	Technical Assistance Support
TAT	Turn around time
TBD	To Be Determined
TCA	Transformational Communication Architecture
TCO	Total Cost of Ownership
TCP-IP	Transmission Control Protocol Internet Protocol
TCU	Total Cost of Utilization
TDA	Technical Design Authority/Agent
TDP	Technical Data Program
TECHEVAL	Technical Evaluation
TECOM	Test & Evaluation Command Training and Education Command
TELEPORT	Telecommunications Portal

TEMP	Test and Evaluation Master Plan
TES	Test and Evaluation Strategy
TESP	Test and Evaluation Strategy Plan
TLCSM	Total Life Cycle Systems Management
TMCR	Technical Manual Contract Requirement
TMINS	Technical Manual Identification Numbering System
TMPE	Test, Measurement, and Diagnostic Equipment
TNOSC	Theater Network Operations and Security Center
TOC	Total Ownership Cost
TPM	Technical Performance Metrics
TPO	Technical Process Owner
TPS	Test Program Sets
TRL	Technology Readiness Level
TRPPM	Training Resources Planning Process Methodology
TRR	Test Readiness Review
TSA	Training Support Agent
TSAT	Transformational Satellite
TSw	Tactical Switching
TTP	Tactics, Training and Procedures
TV	Technical View
TYCOM	Type Command
UC	Underpinning Contract
UCDMO	Unified Cross Domain Management Office
UDOP	User-Defined Operational Picture

UID	Unique [Item] Identification
UJTL	Universal Joint Task List
ULSS	User's Logistics Support Summary
UNIX	Universal Network Information Exchange
uNNPI	Unclassified NNPI
uNTPP	Unclassified Transportation Network Protection Policy
UPS	Uninterruptible Power Supply
USAF	United States Air Force
USB	Universal Serial Bus or Port
USGS	U.S. Geological Survey
USMC	United States Marine Corps
USN	United States Navy
USNO	U.S. Naval Observatory
USSTRATCOM	United States Strategic Command
VDS	Virtual Directory Services
VOI	Value on Investment
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VSSD	Very Small Site Design
VTC	Video Teleconferencing
WAN	Wide Area Network
WBS	Work Breakdown Structure
WFNS	Warfighter Network Services
WGS	Wideband Gapfiller System

WINS	Windows Internet Naming Service
WIN-T	Warfighter Information Network – Tactical
WIP	Work In Progress
WIPT	Working IPT
WMD	Weapons of Mass Destruction
XML	Extensible Markup Language